FortiGate – Final Project

Samuel Kim

Full Name: Samuel Kim

Assign: NSE-Fortinet Firewall

Lecturer: Yosef Baruch EL

Date of Submission: 7.3.2024

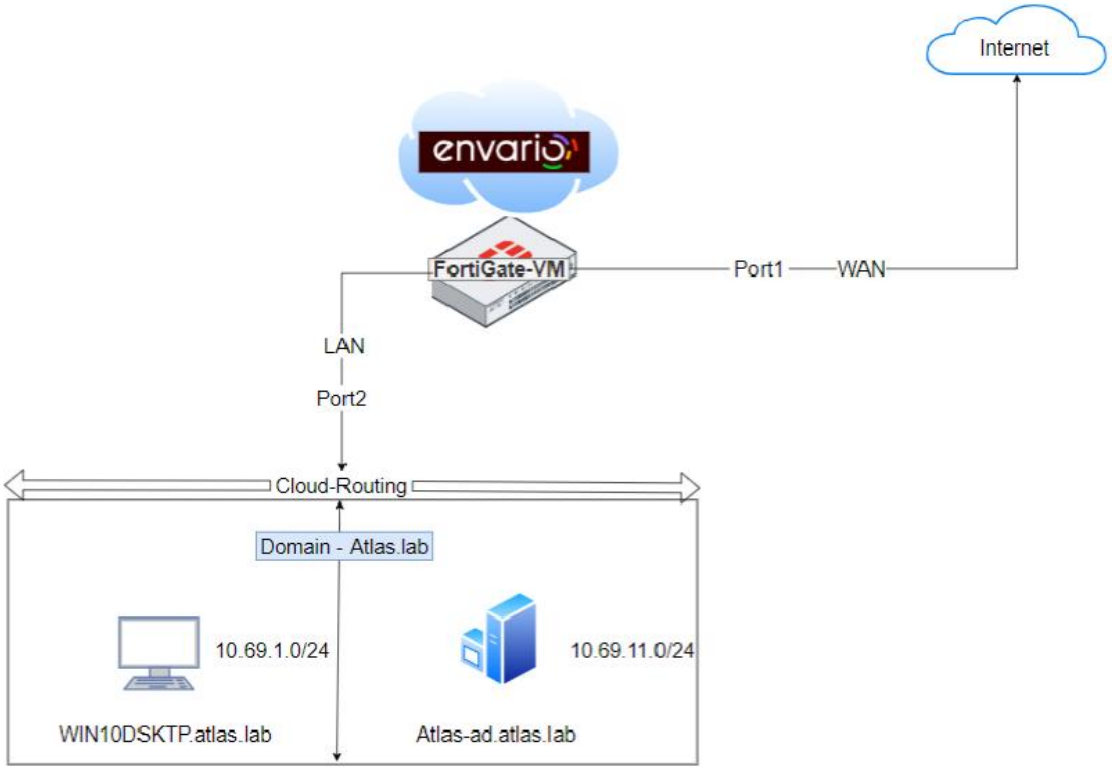
Table of Contents

Topology

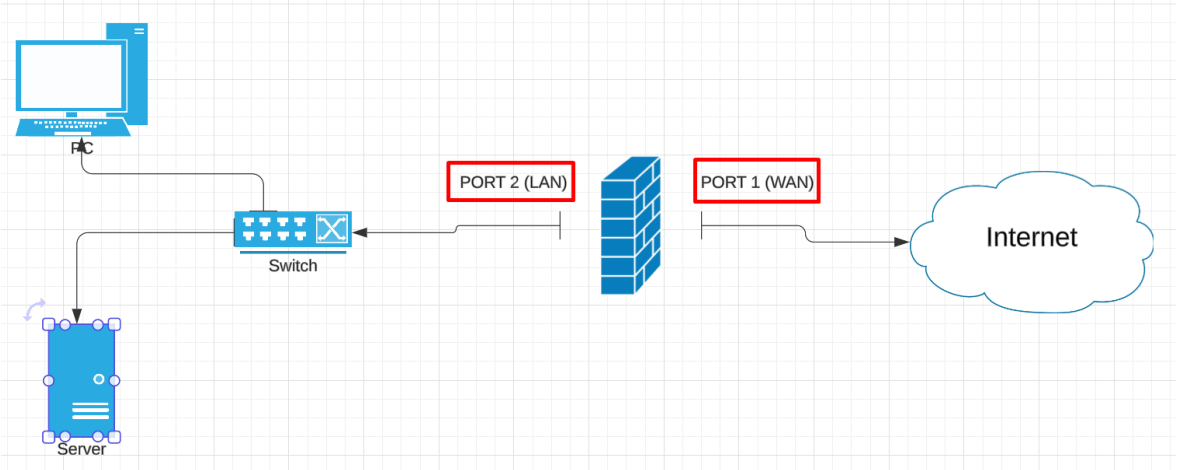
In this work we will use virtual machines on the ENVARIO website. Now let's talk about topologies.

We have a topology that contains a local network that goes to the WAN through FORTIGATE

On the local network we have two different sub masks, one client computer and a server.



we will use two ports that are located on the device itself, "Port 2" goes to the local network and the second port "Port 1" to an external network or through an Internet provider, to a global network called the Internet.



What is FortiGate?

FortiGate is a series of network security appliances developed by Fortinet, a cybersecurity company. FortiGate appliances provide various security features such as firewall, virtual private network (VPN), intrusion prevention, antivirus, content filtering, and application control. These appliances are designed to protect networks from a wide range of threats, including malware, hacking attempts, unauthorized access, and other cyber-attacks.

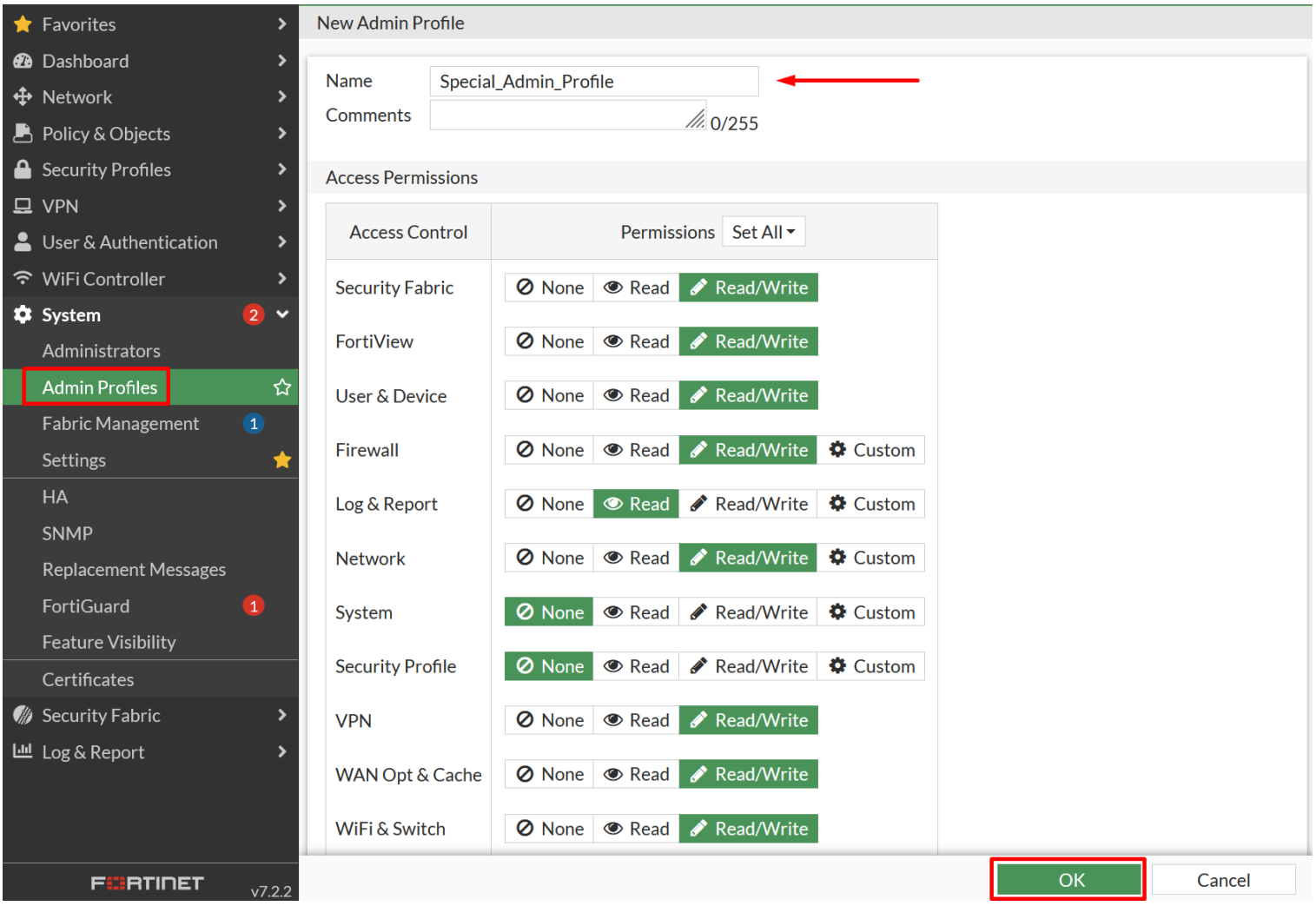
Where is it used?

FortiGate appliances are widely used in enterprise networks, data centers, and service provider environments to secure network traffic and ensure the confidentiality, integrity, and availability of data and resources. They are available in various models and configurations to meet the specific security needs of different organizations, from small businesses to large enterprises.

User Management

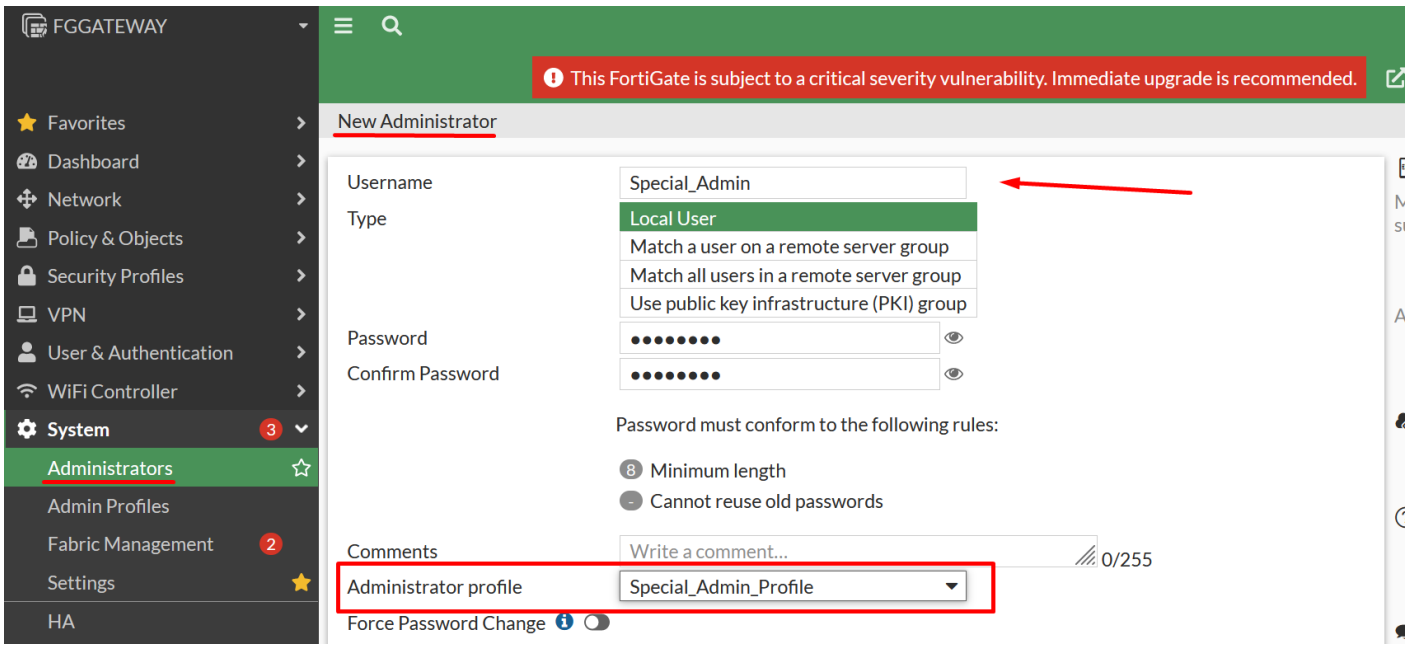
- Create a new profile (with the name you decide) with similar privileges to the Super_admin profile.

We go to the administrative profiles tab and create a new one. It will be like a Super profile, but I will limit it in some functions like: Log & Report: Only reading, And I will hide tabs such as system and Security Profiles

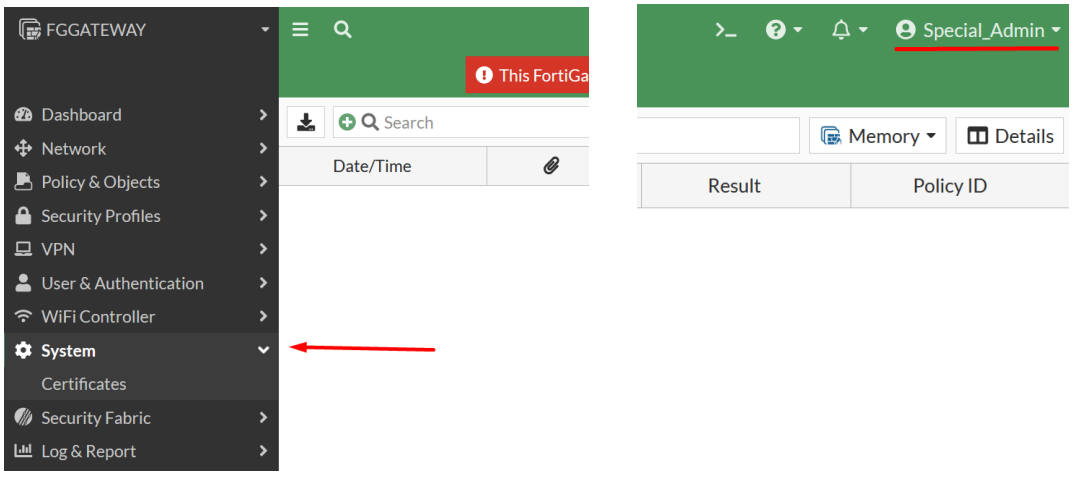


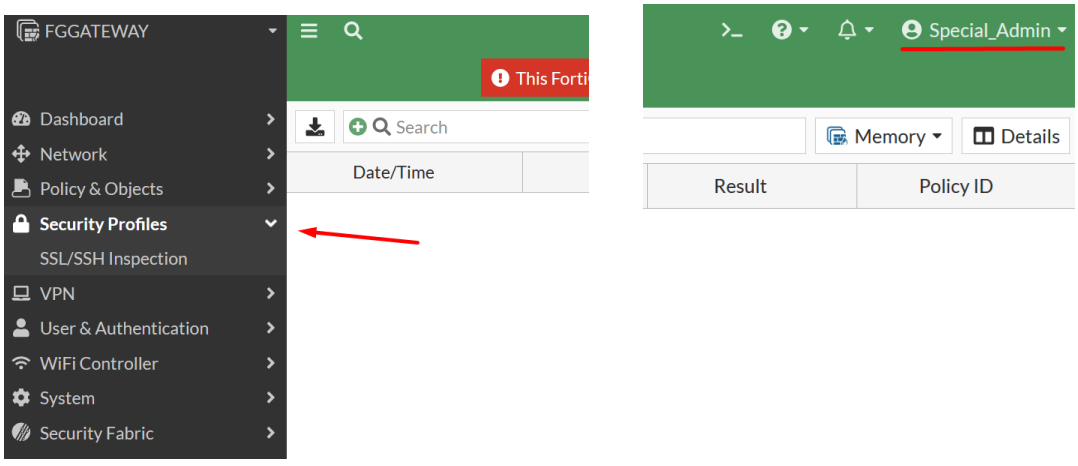
- Create a new user (with the name you decide) This user must be added to the newly created group (with Super_admin privileges)

Now we will create a new administrator user and give him the profile that we created before



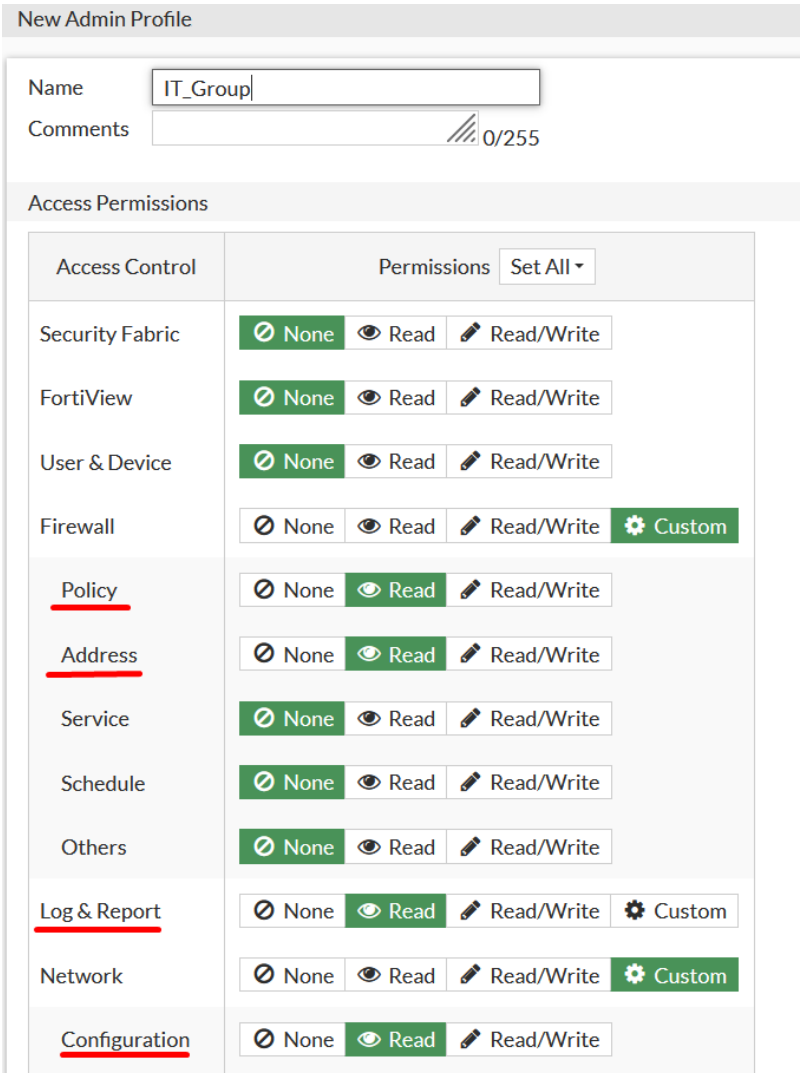
Now we go to a new profile, and as you can see that it is limited.





- Create a new group, must be created for IT with viewing privileges only “ Policy, logs, VIPS, interfaces ”

We are creating a new profile \ group - for the IT department as well as 3 users and giving them read-only permission to specific tabs.

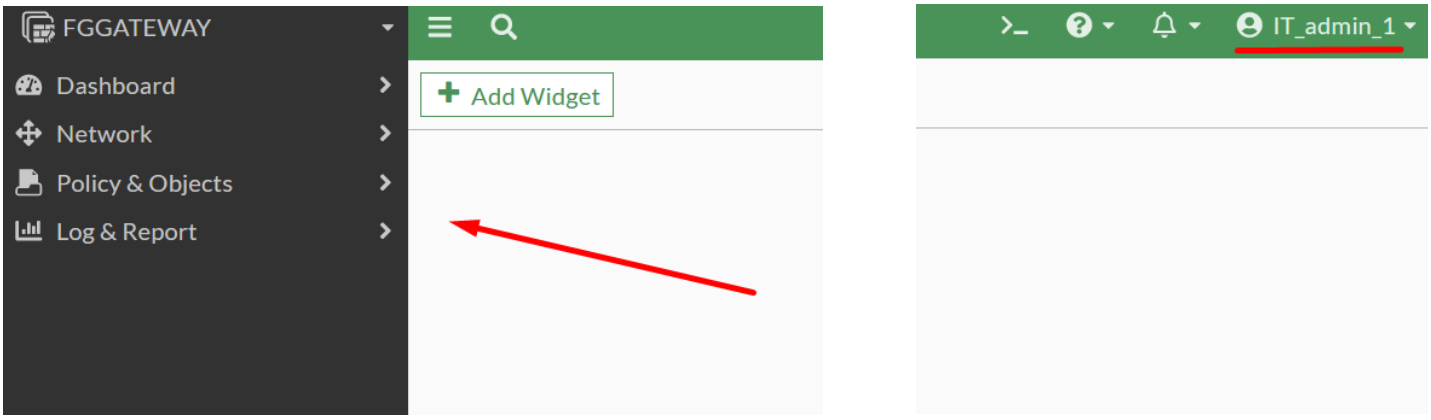


- Create 3 new users and add them to this group.

Name	Trusted Hosts	Profile
System Administrator 6		
IT_admin_1		IT_Group
IT_admin_2		IT_Group
IT_admin_3		IT_Group

Here we see that many tabs are not accessible to them, and those that they have access to are available only with Read permission.

"Read permission" refers to the access level granted to users for just viewing configuration settings but not modify.



Password Policy

- Password policy must be created for all users.

At least 8 characters are required

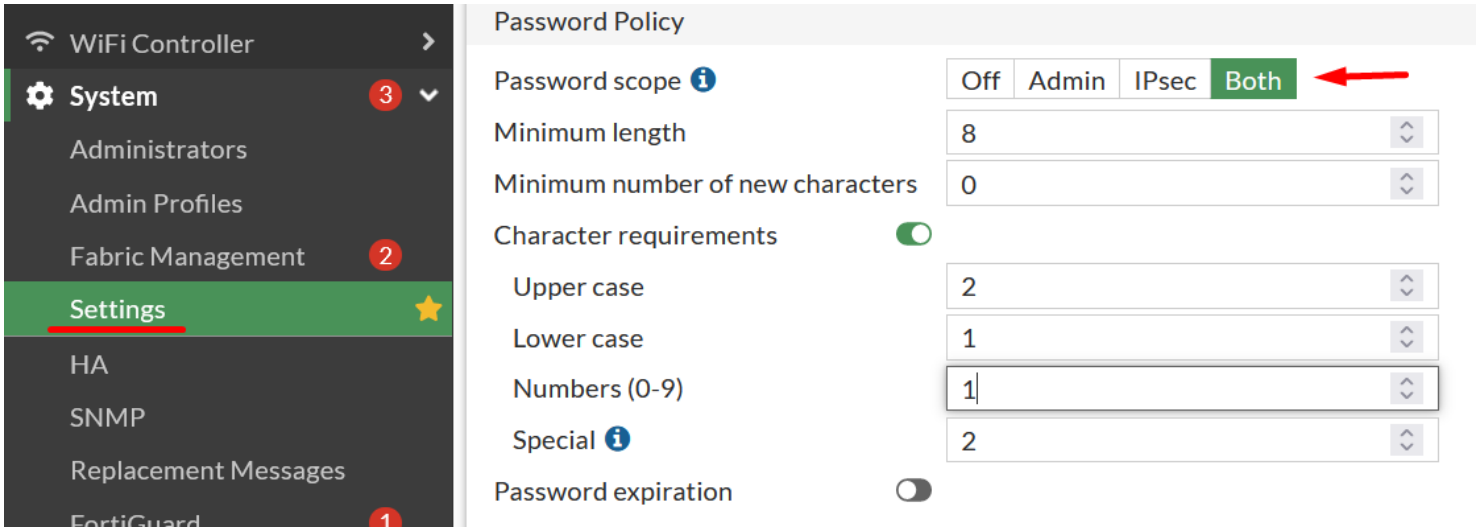
2 special symbols

2 large letter

1 small letter

1 number

You need to be responsible when you are choosing a password in order to protect the system from external threats & Password hacking such as - Dictionary attacks, Brute force attacks, Weak password attacks and etc.



VPN: SSLVPN Tunnel Mode

- A tunnel connection must be created with LADP - based users.

1. Create a group named LDAP_Sales

2. Create 3 new users and add them to the LDAP_Sales group

3. A policy must be established that will allow VPN users to access Win10 via RDP

4. Attach documentation of connecting to the user in RDP by VPN

What is SSL

SSL is Secure Sockets Layer. It's a standard technology that ensures encrypted communication between a web server and a browser.

SSL is commonly used to secure data transmission over the internet, such as sensitive information entered on websites (like passwords or credit card numbers).

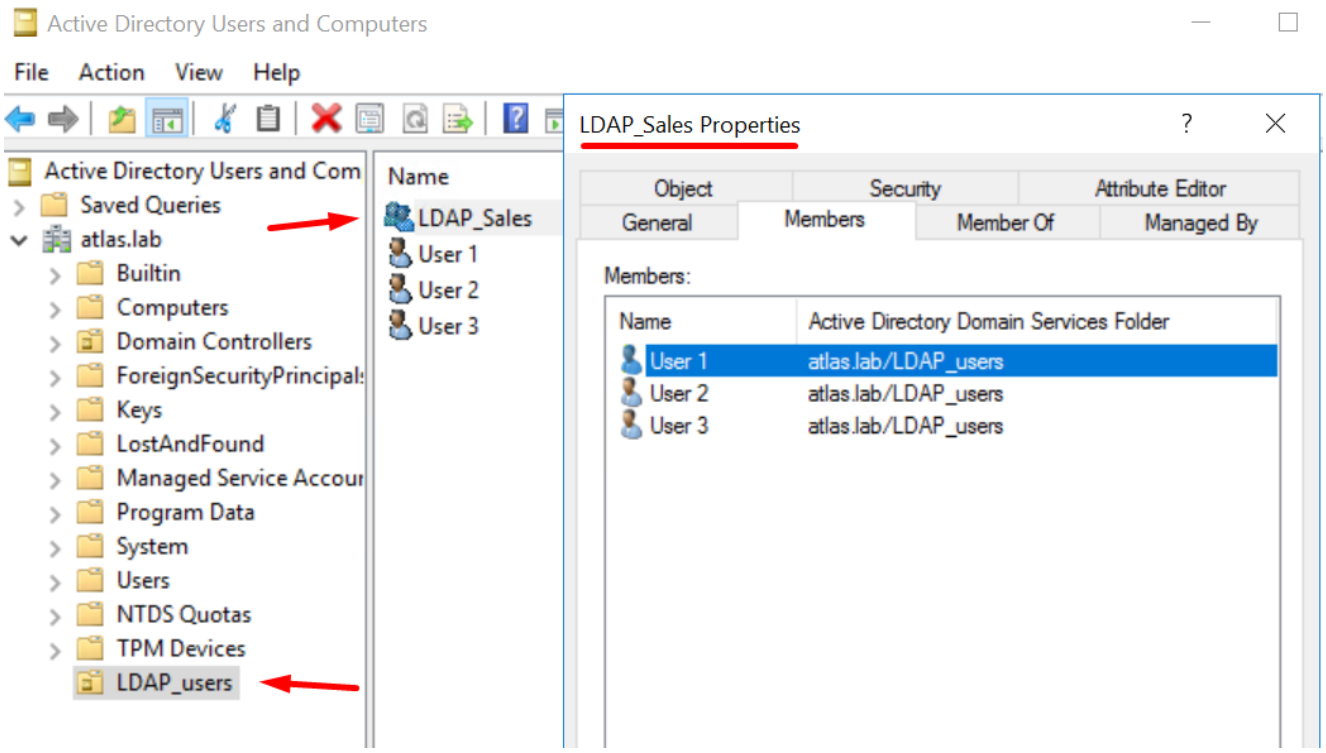
What is Tunnel Mode

SSLVPN tunnel mode in FortiGate establishes a protected and encrypted link between an individual's device and the company's network.

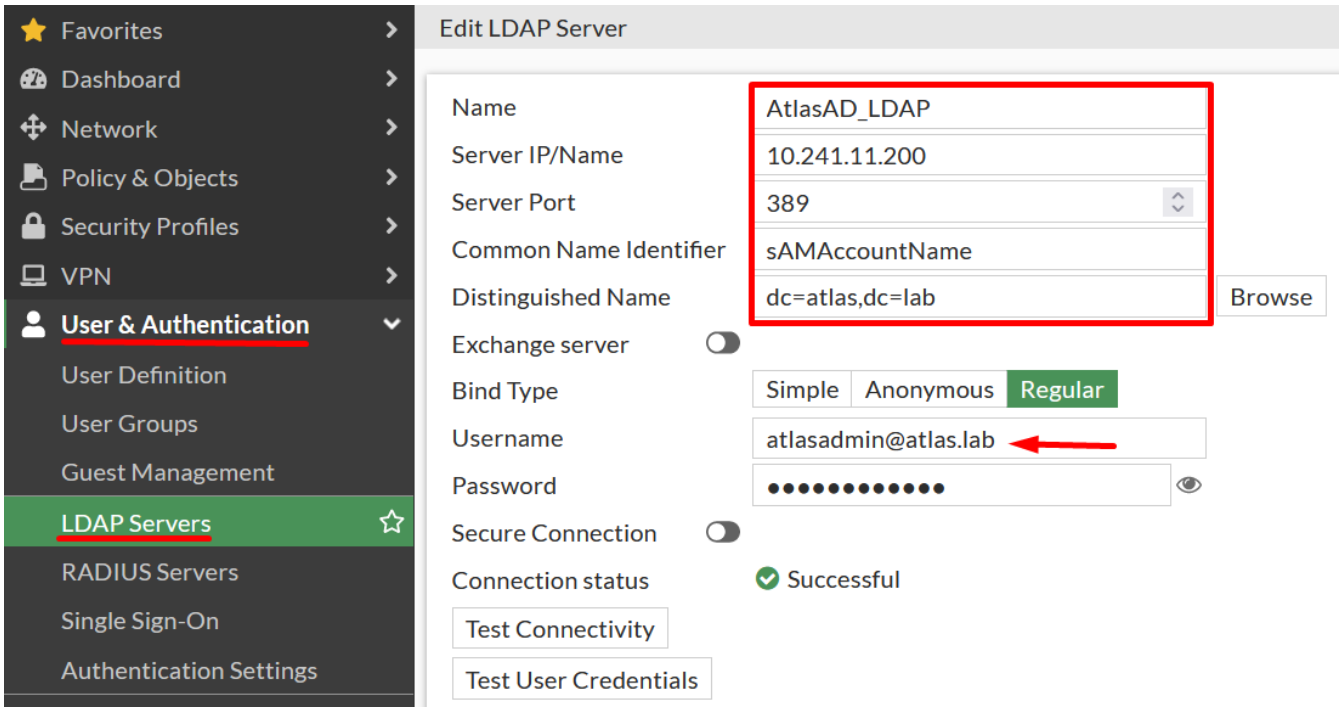
In our case, this will help us to connect users from the Active Directory so that they can connect to devices using the RDP protocol via VPN

It permits remote users to securely connect to internal resources, bolstering security for employees working from afar and safeguarding the secrecy of valuable data.

We will create a group and three new users in the Active Directory on the AtlasAD server.

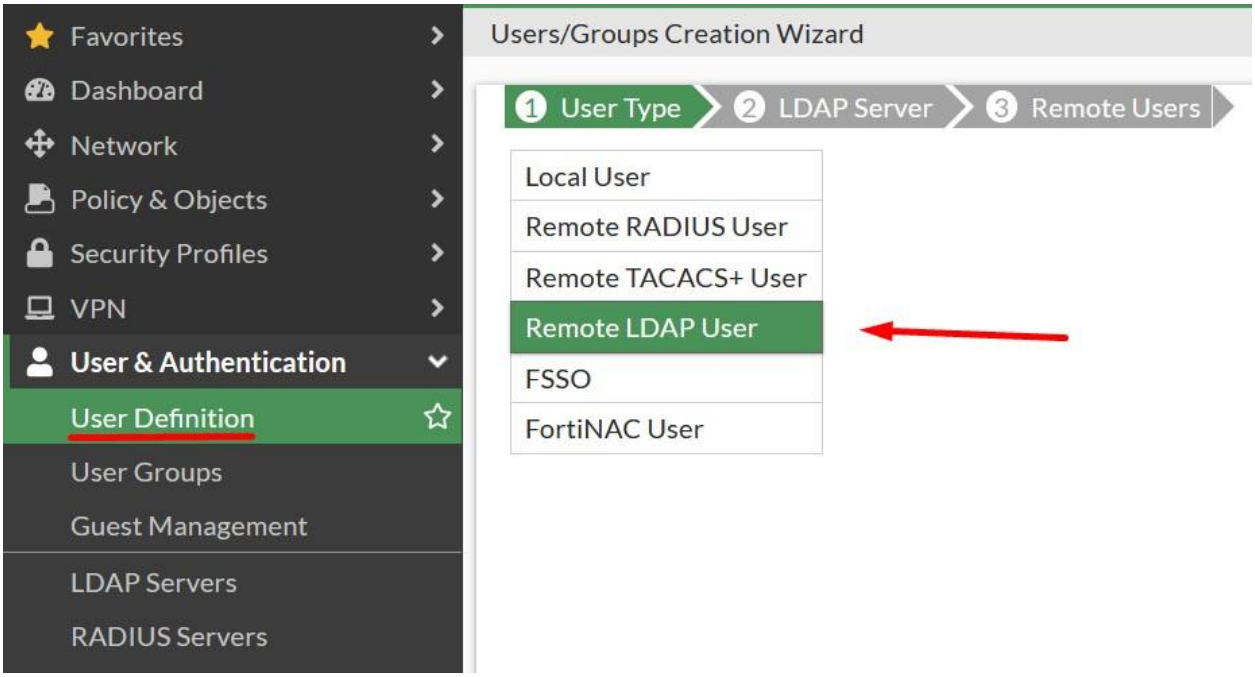


Now we are moving to FortiGate and we will connect the LDAP server to Firewall

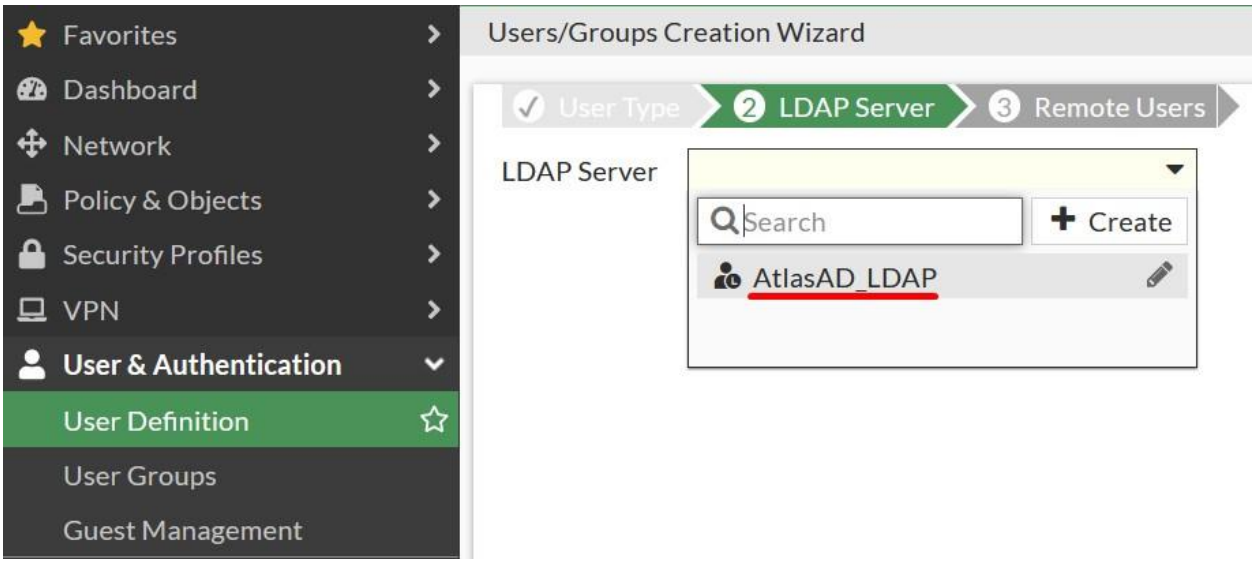


I connected the Atlas server to Fortigate, adding his IP address, username and password of the server administrator (UPN) , domain component – dc=atlas,dc=lab and how you can see that we have a connectivity between them.

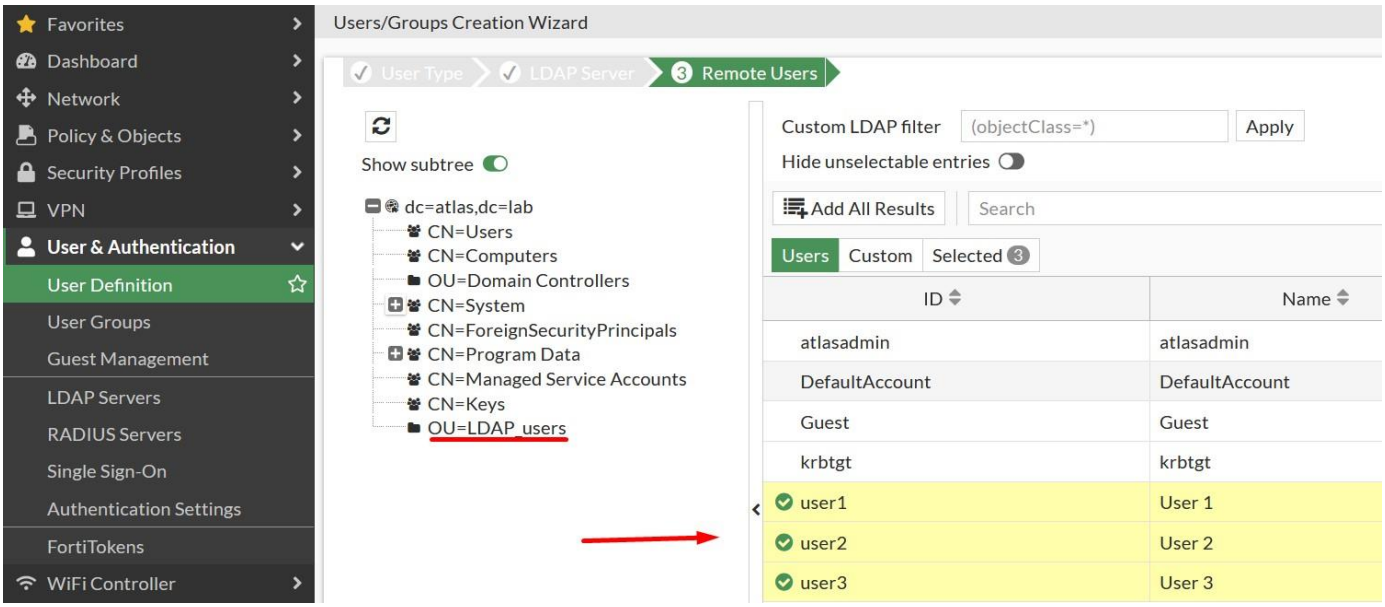
Now we will connect new users from the Active Directory to Fortigate



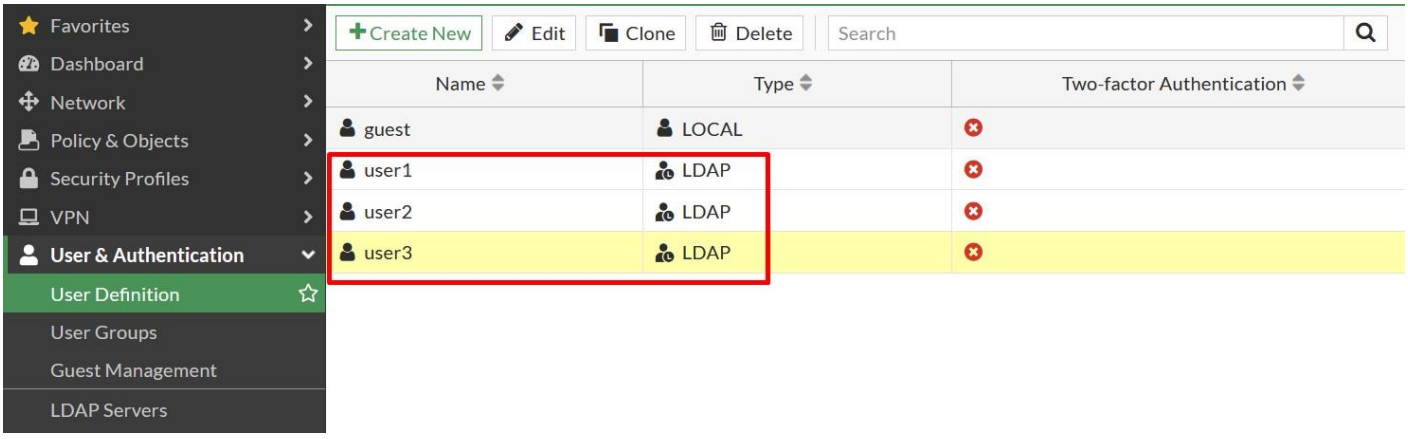
Choose our server.



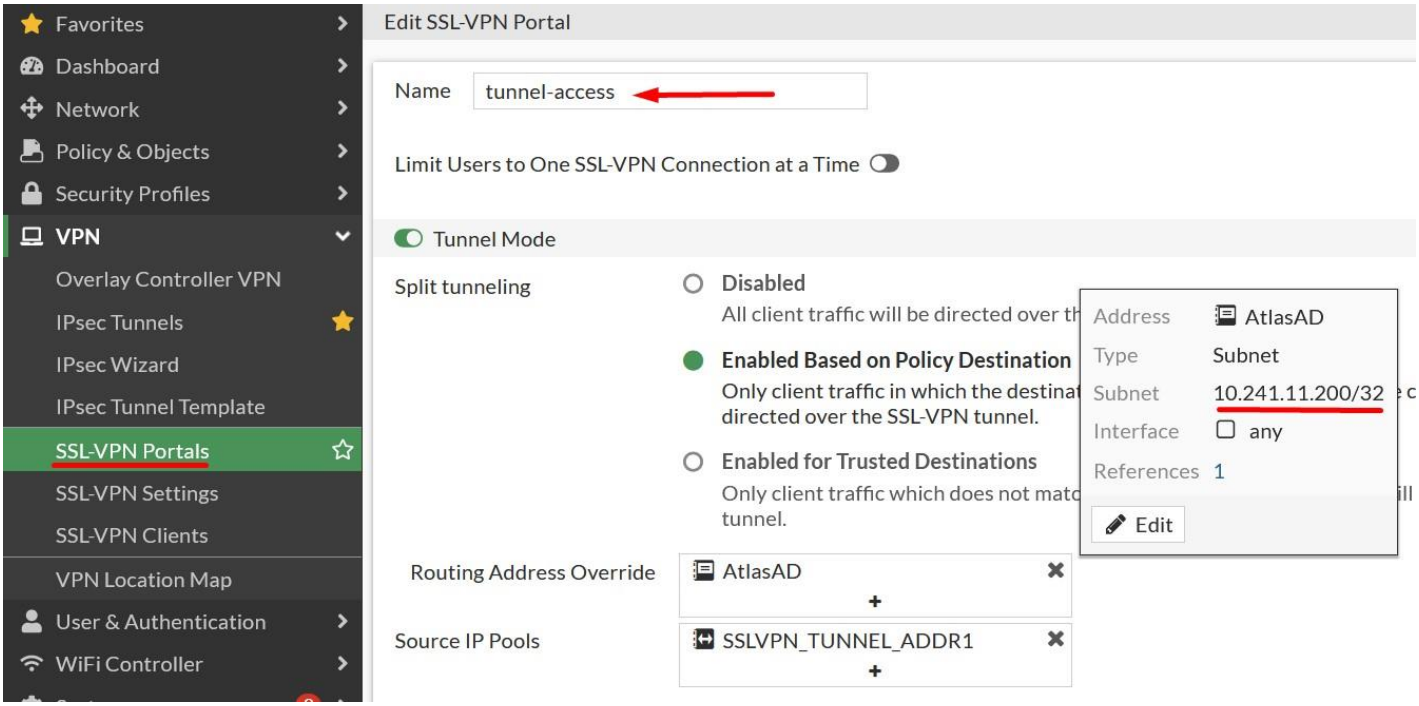
Next we need to select new users from the Active Directory

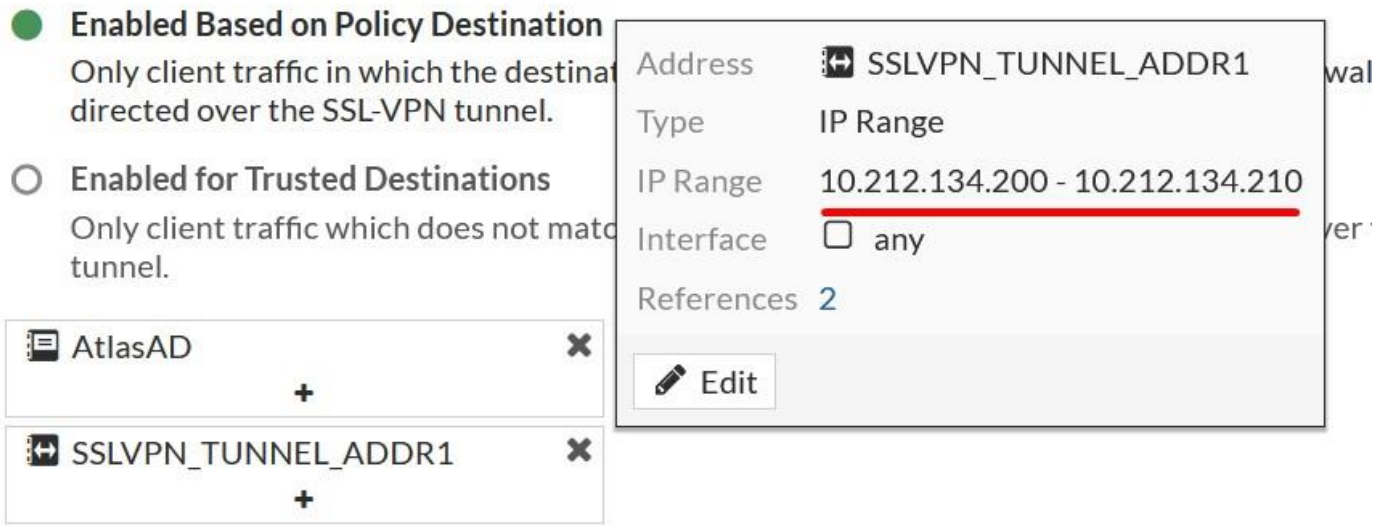


And check that they have been added to the user category

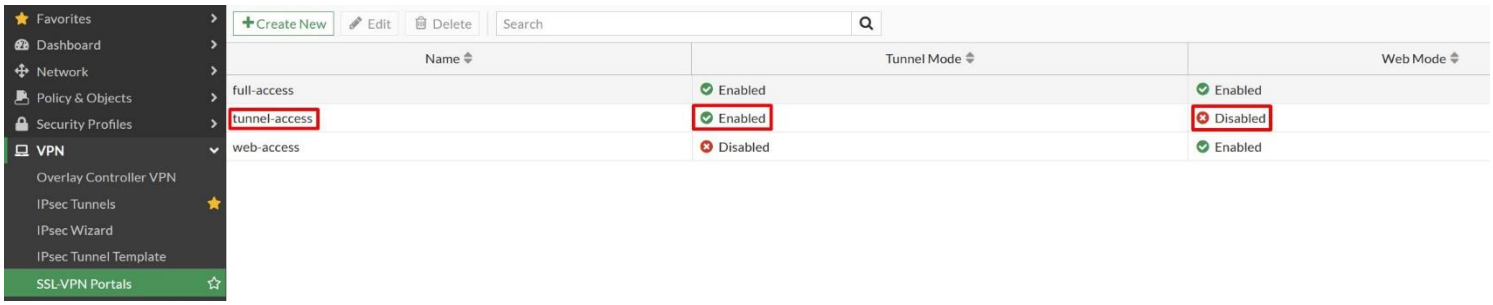


Next, we need to create a tunnel portal, select the Atlas server address, add a pool of addresses with which clients will connect and select SPLIT TUNNELING mod on so that all traffic from an external computer does not go only through the Fortigate.

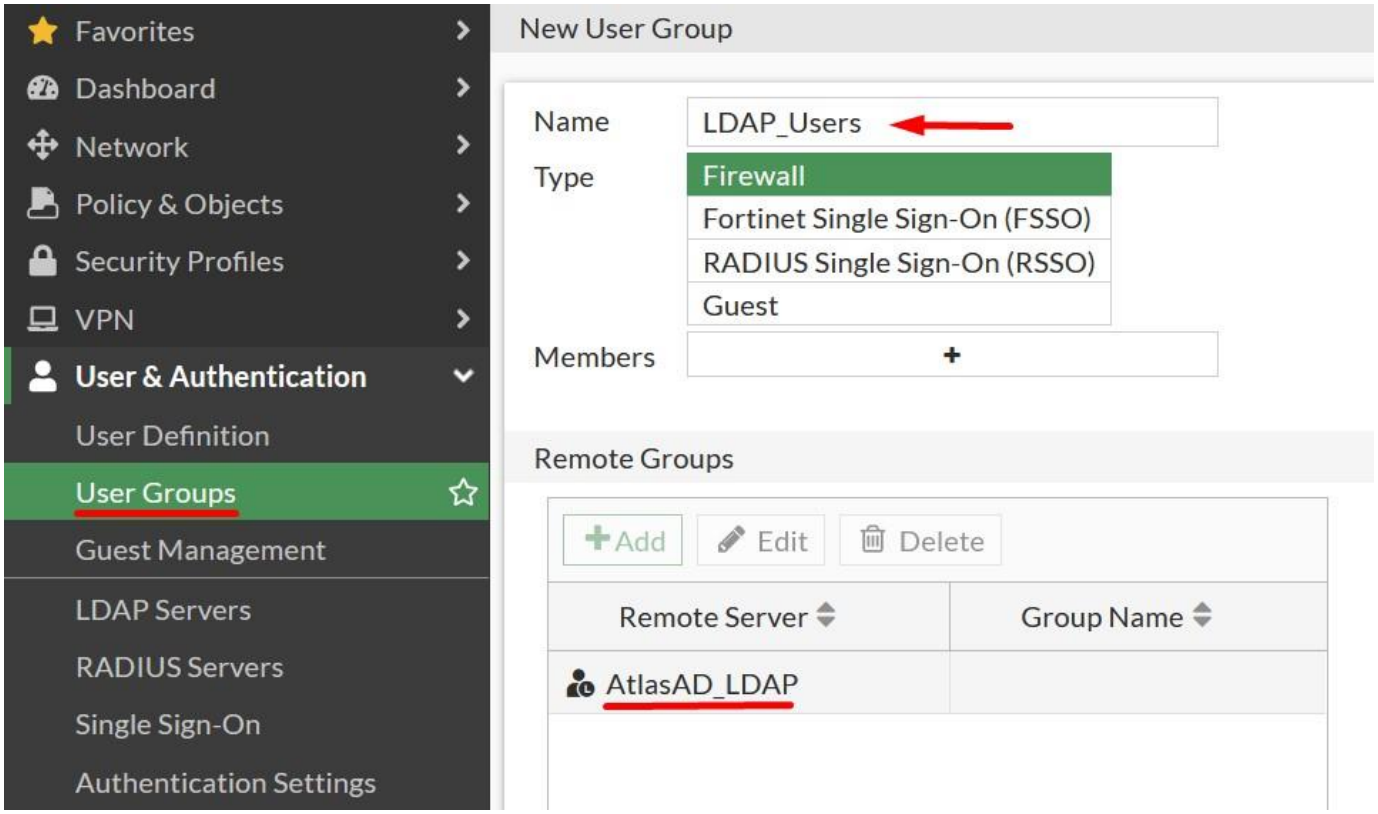




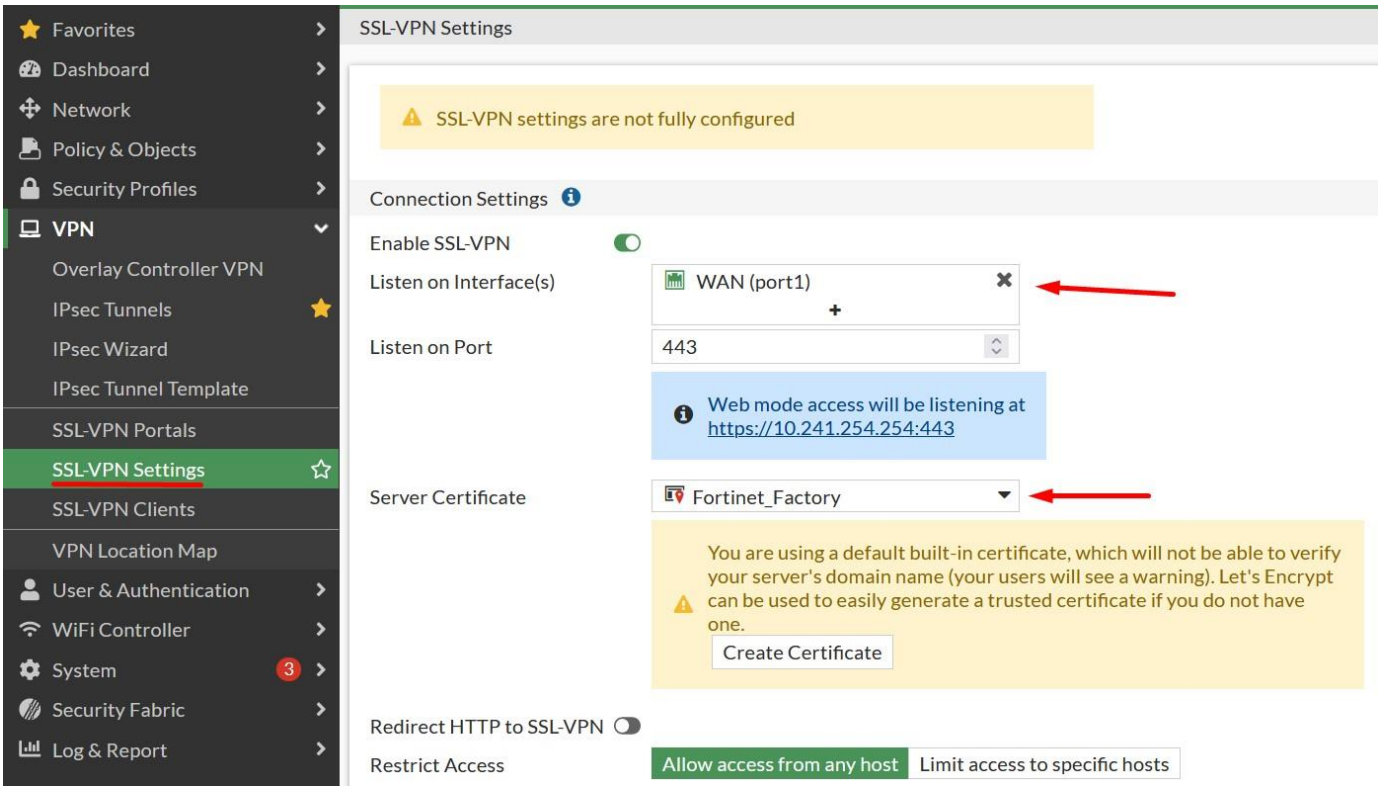
Everything is set up and we will move on to the next steps



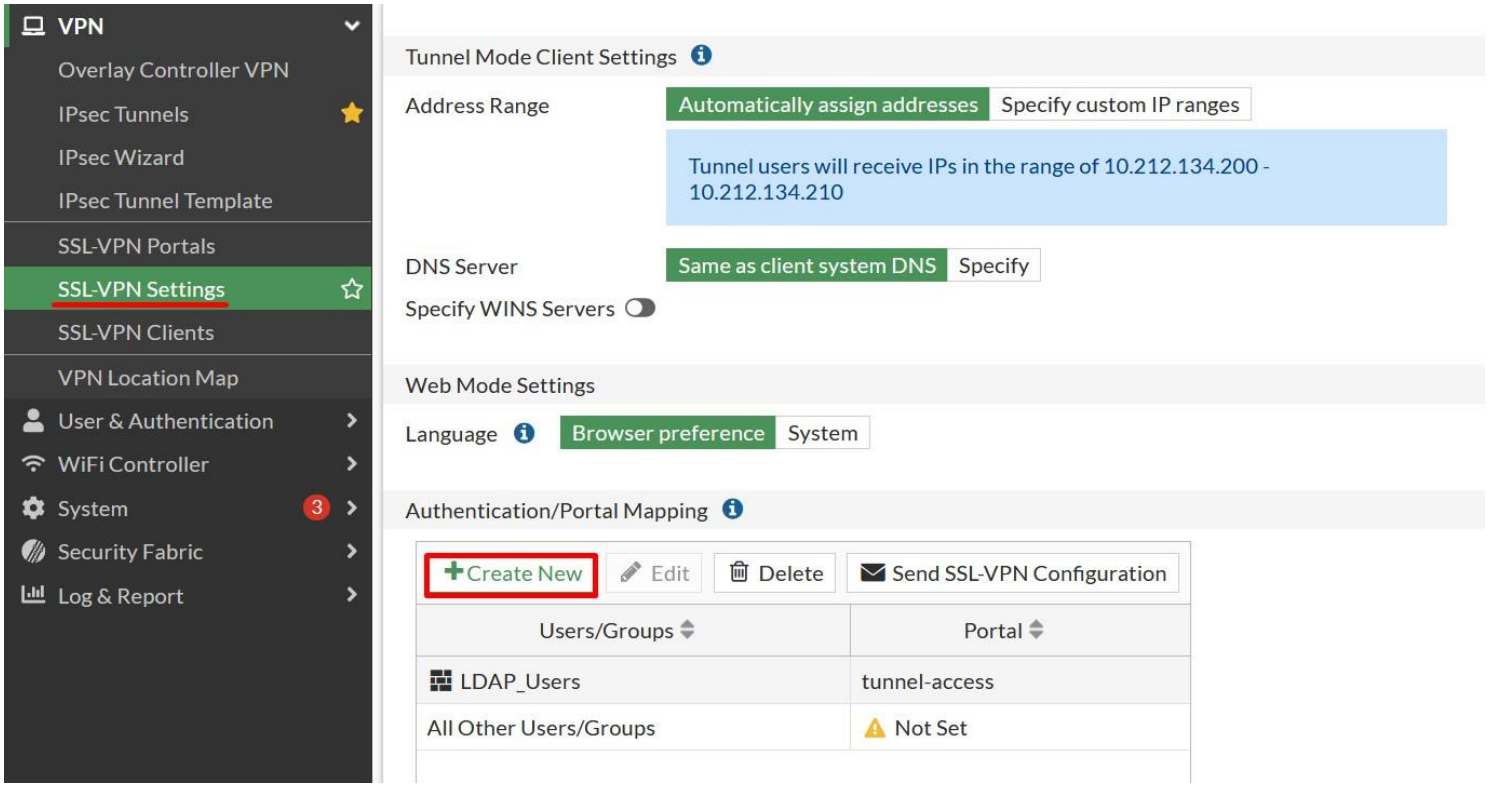
Now we need to add the user group that we created from the Active Directory in FG

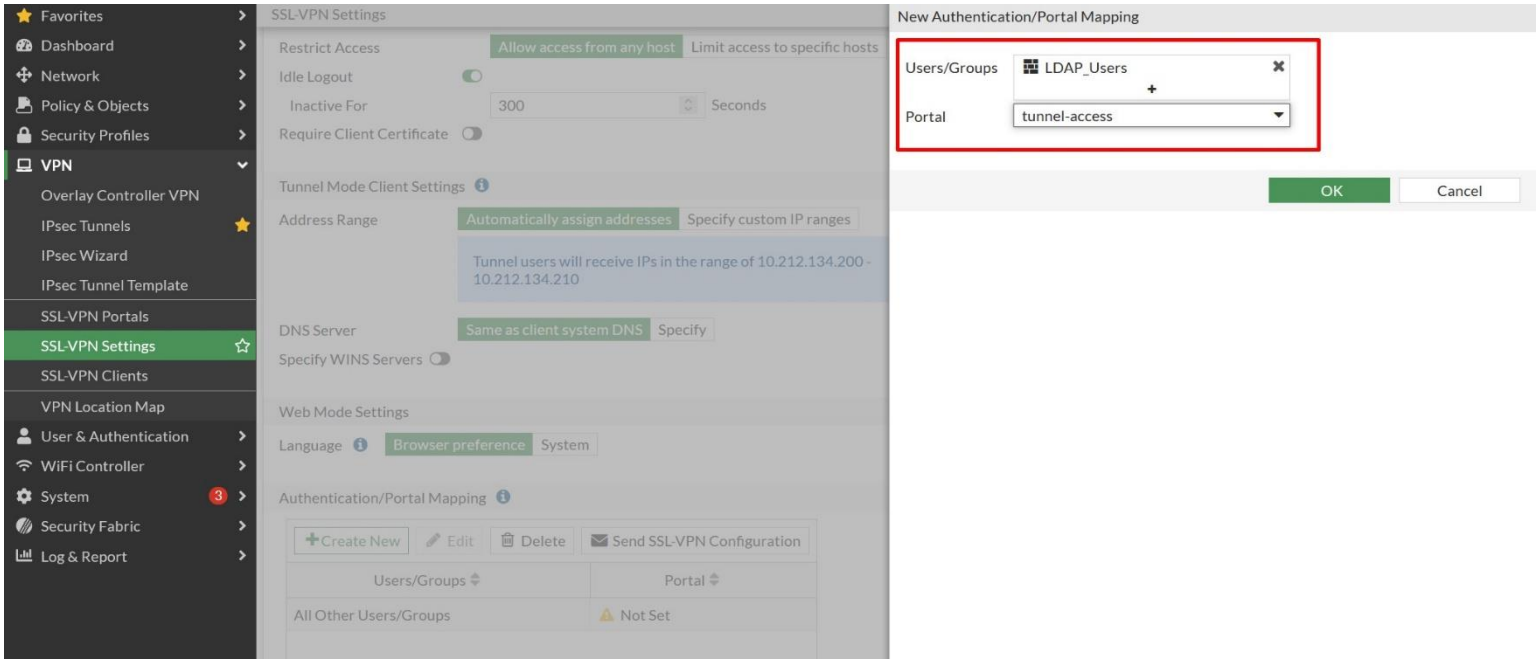


I'll go to the VPN settings, select the port from which traffic will flow, in our case the external WAN port, we also select an SSL certificate



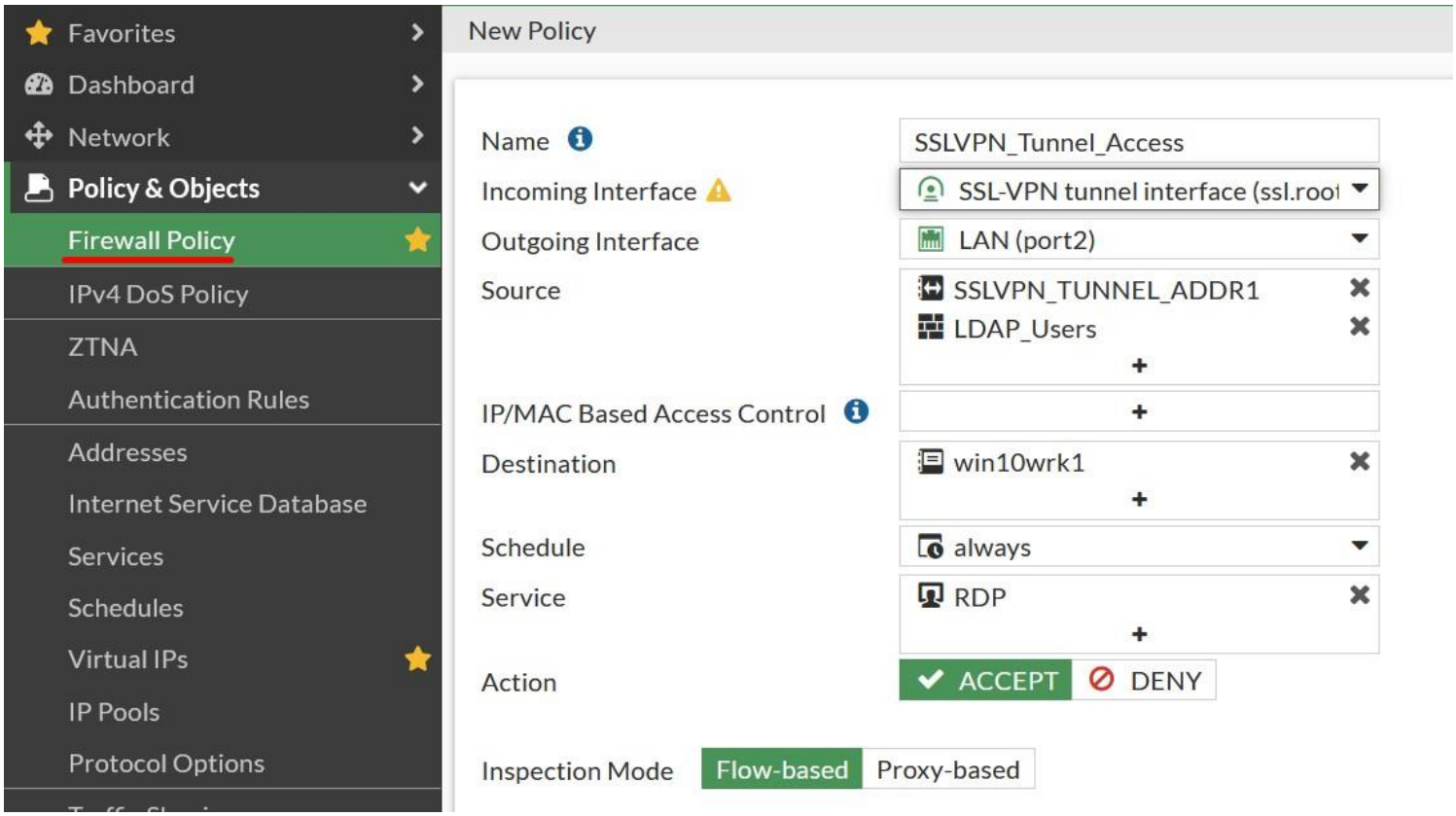
Select our LDAP users and the portal to which they will connect.





Without a configured policy, our Remote Access to PC via VPN will not work, so let's configure it now.

Let's move to the policy category and create a new rule, give a name and designate which port the traffic will go to - select the tunnel port that we created, in which "PORT 1" is designated - WAN, and it will redirect the traffic to the LAN, to our PC. Next, we select users from the Active Directory as well as the pool of addresses with which they will connect, the destination will be the PC and the RDP service (Remote Desktop Protocol)

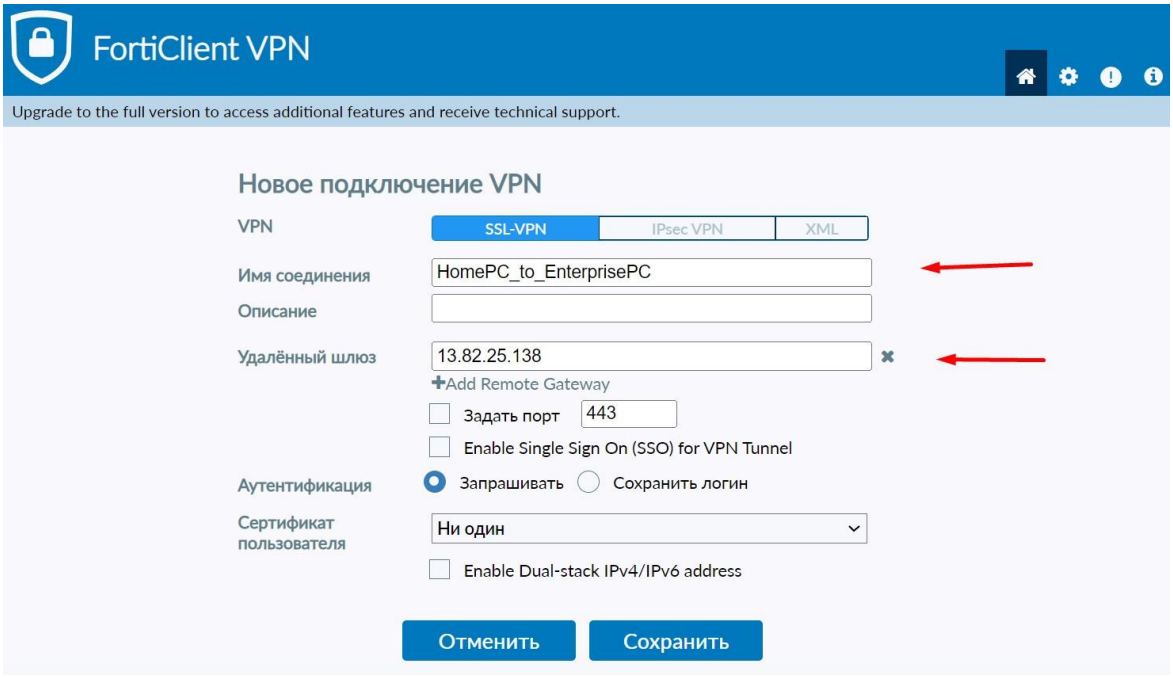


Let's check if its works.

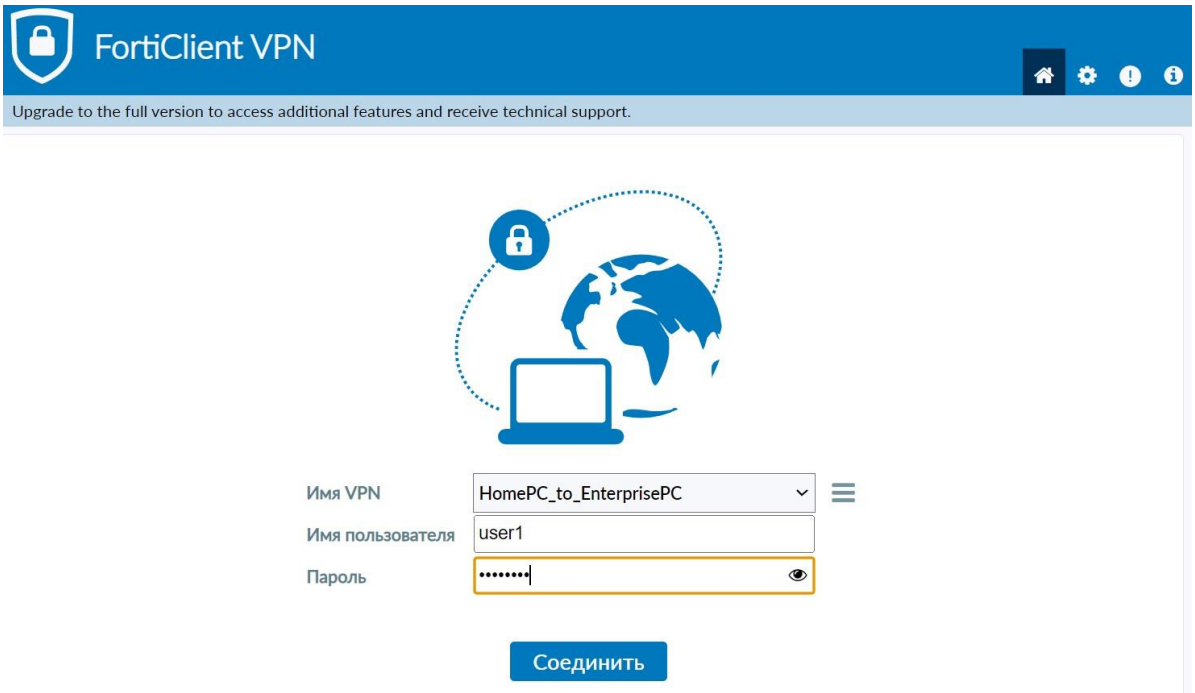
First, we need to install the FortiClient VPN on the computer to connect remotely and safety to the workstation.

I apologize for the Russian language; it was not possible to change it to English

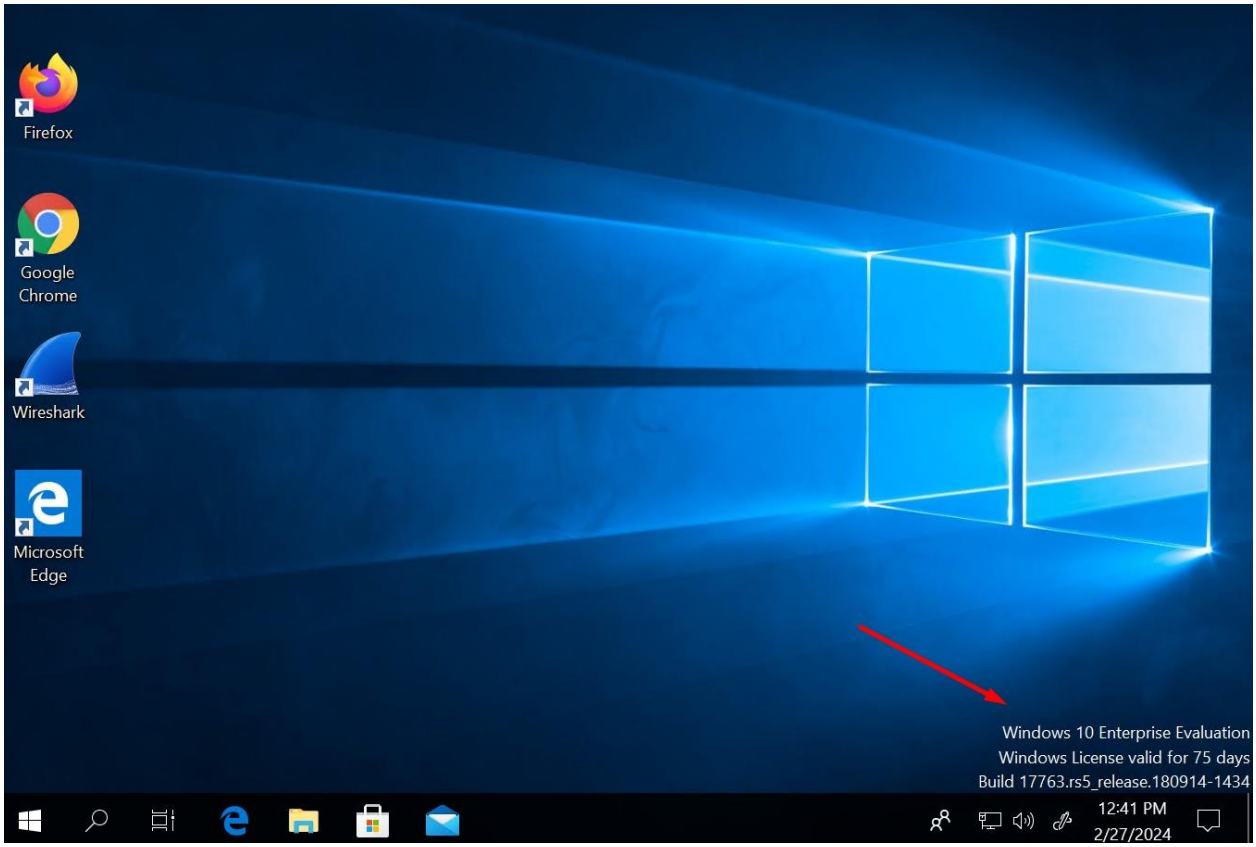
We give the name of our session, in our case it is from a home PC to the company's workstation, we register the remote Default Gateway of FortiGate, where the traffic will flow. After this, we leave the default port 443/HTTPS since we did not change it in the SSLVPN settings.



After, we select our newly configured VPN, we write the username from the Active Directory and its password.



And how can we see that the VPN connection is working and we were able to connect via RDP to our remote working environment



How RDP and VPN works?

RDP is a protocol developed by Microsoft that allows users to access and control a computer remotely over a network connection. RDP works by passing the graphical user interface (GUI) of a remote computer to the client and relaying user input back to the remote system. It operates over TCP/IP and typically uses port 3389.

RDP can also be used over a VPN connection to enhance security by encrypting data transmission between the client and the remote system, thereby ensuring confidentiality and integrity. VPNs create secure, encrypted tunnels over public networks such as the Internet, providing an additional layer of security for RDP sessions.

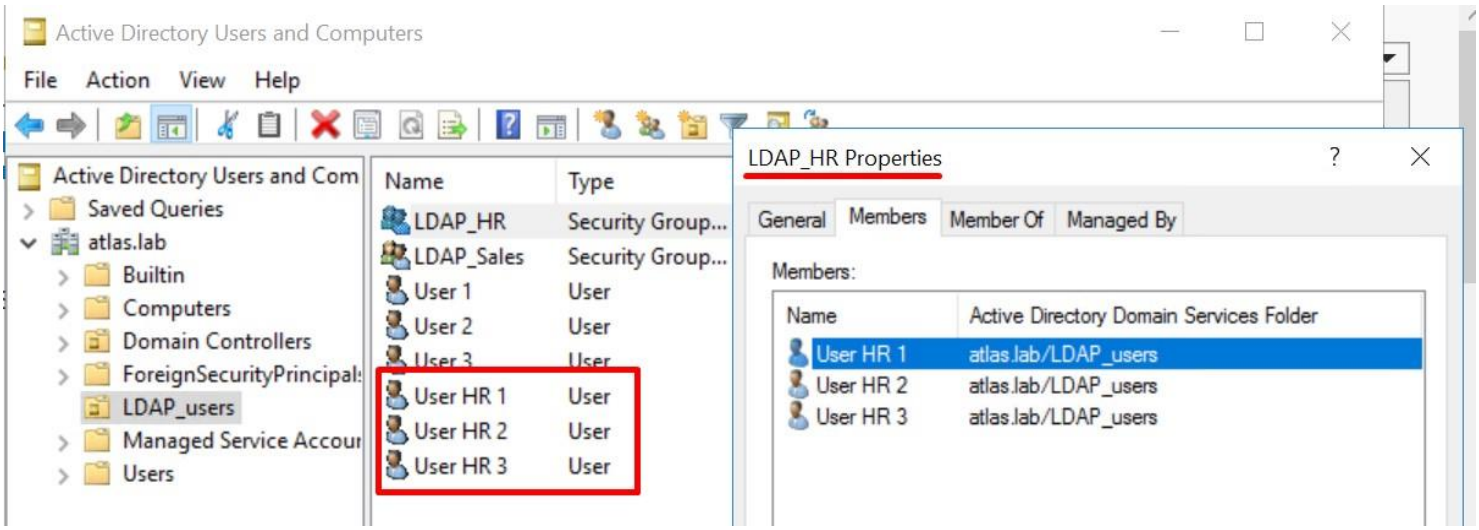
VPN: SSLVPN Web Mode

- A connection must be created in the Web Access configuration with established LDAP users.

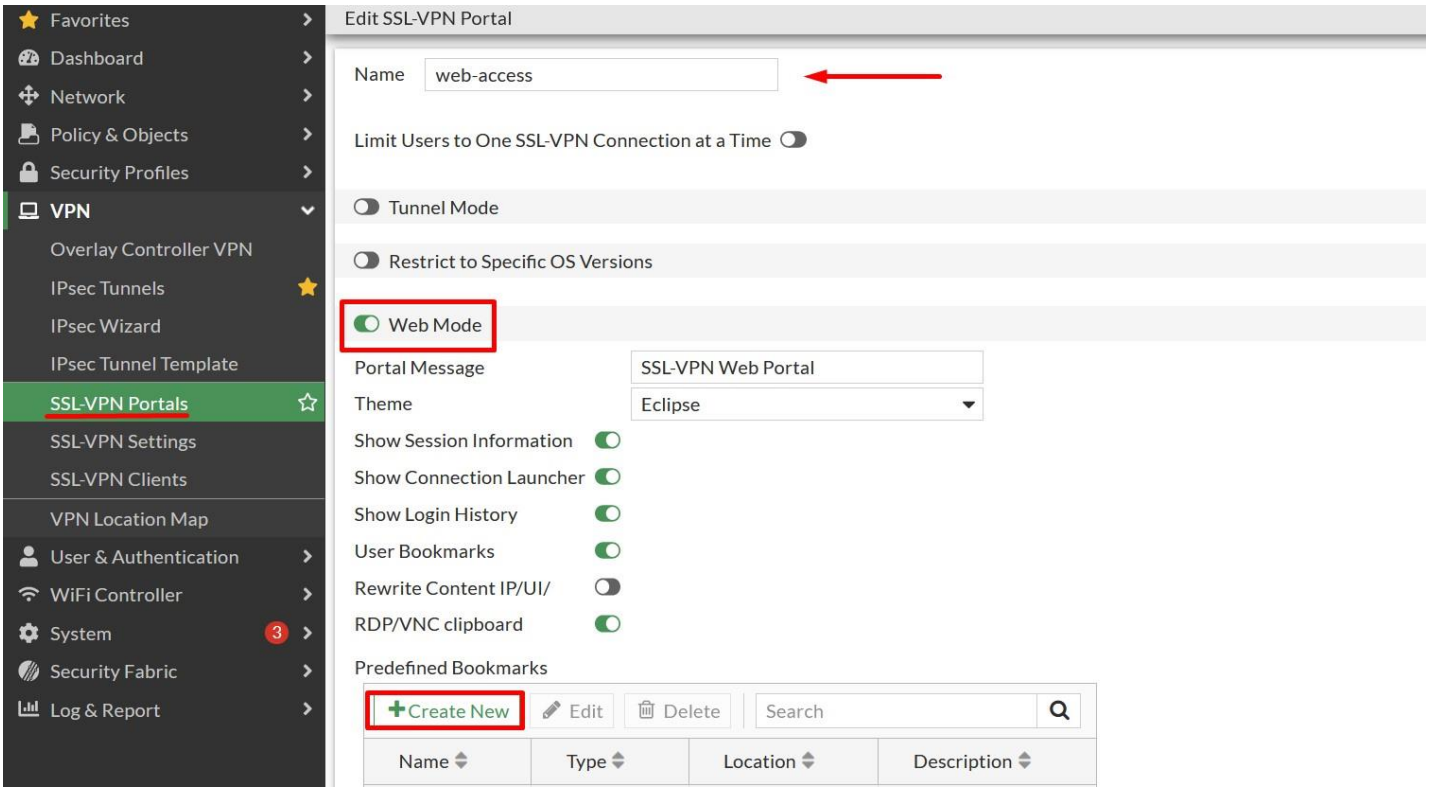
1. Create a group called LDAP_HR
2. Create 3 new users and add them to the LDAP_HR group
3. A law must be created that will allow these users to RDP to Win10

This time we will repeat all our actions but we will connect our users directly through the WEB BROWSER

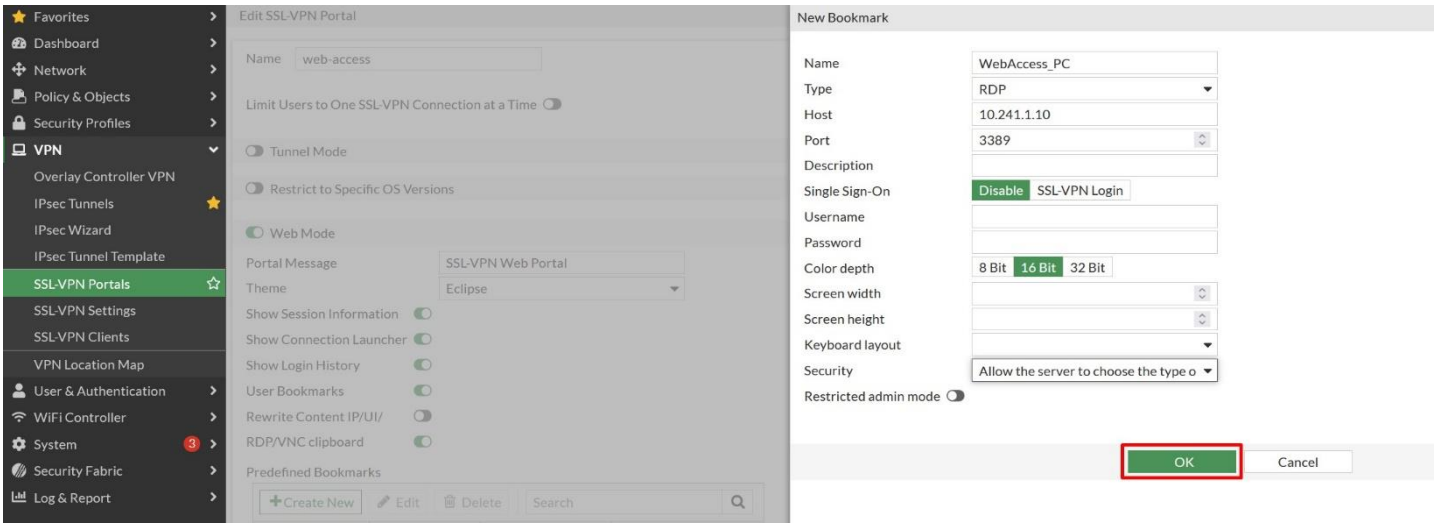
First, let's go to the Active Directory and create new users and add them to the group. (LDAP_HR)



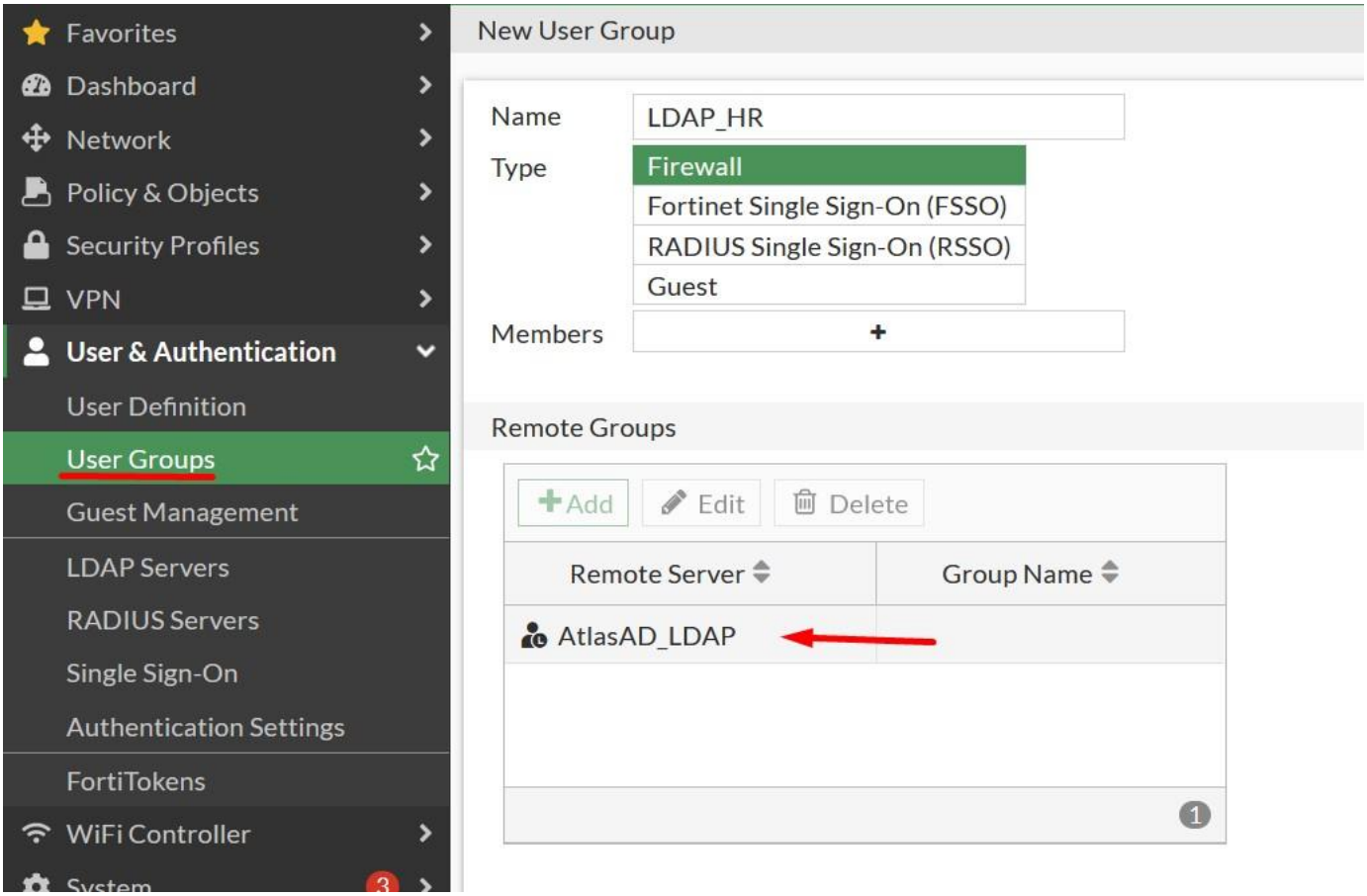
Now we will need to go to the portal settings itself, select Web Access



Now we create a new bookmark, select the RDP service, the address of our workstation (PC), the RDP port and the security type so that it allows the server to choose.

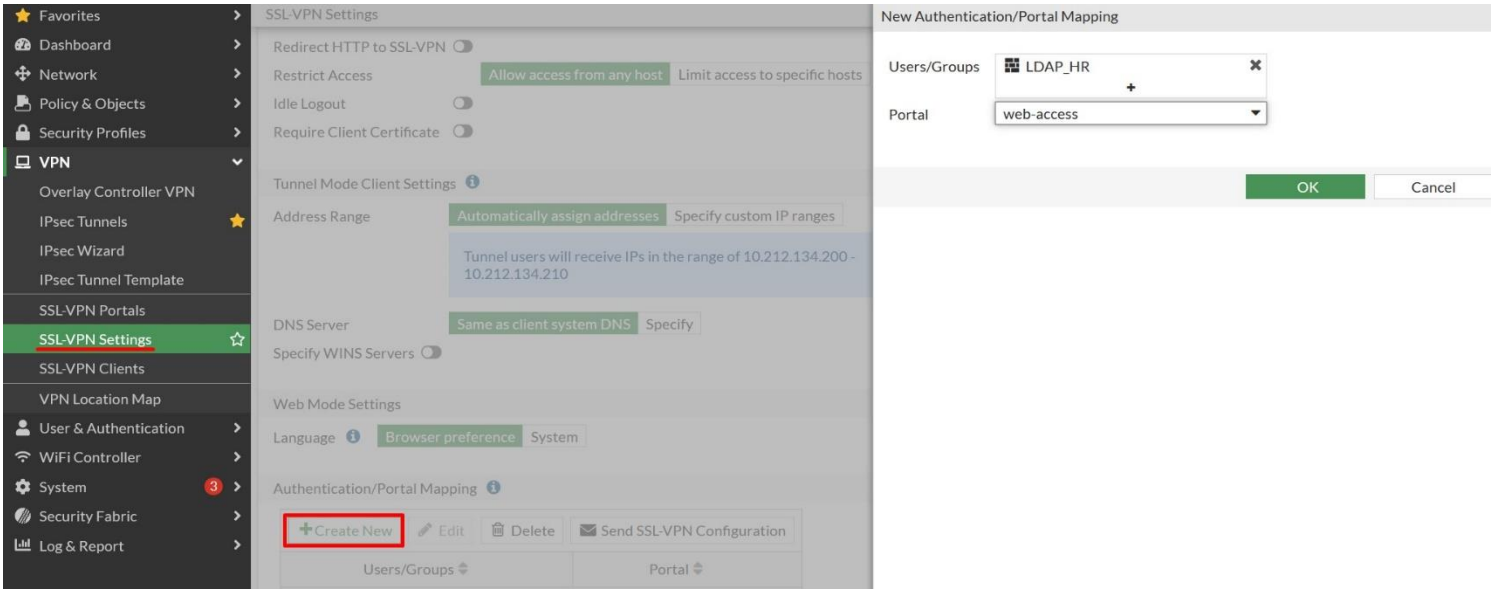


Next, we are adding previously created users from AD to Fortigate

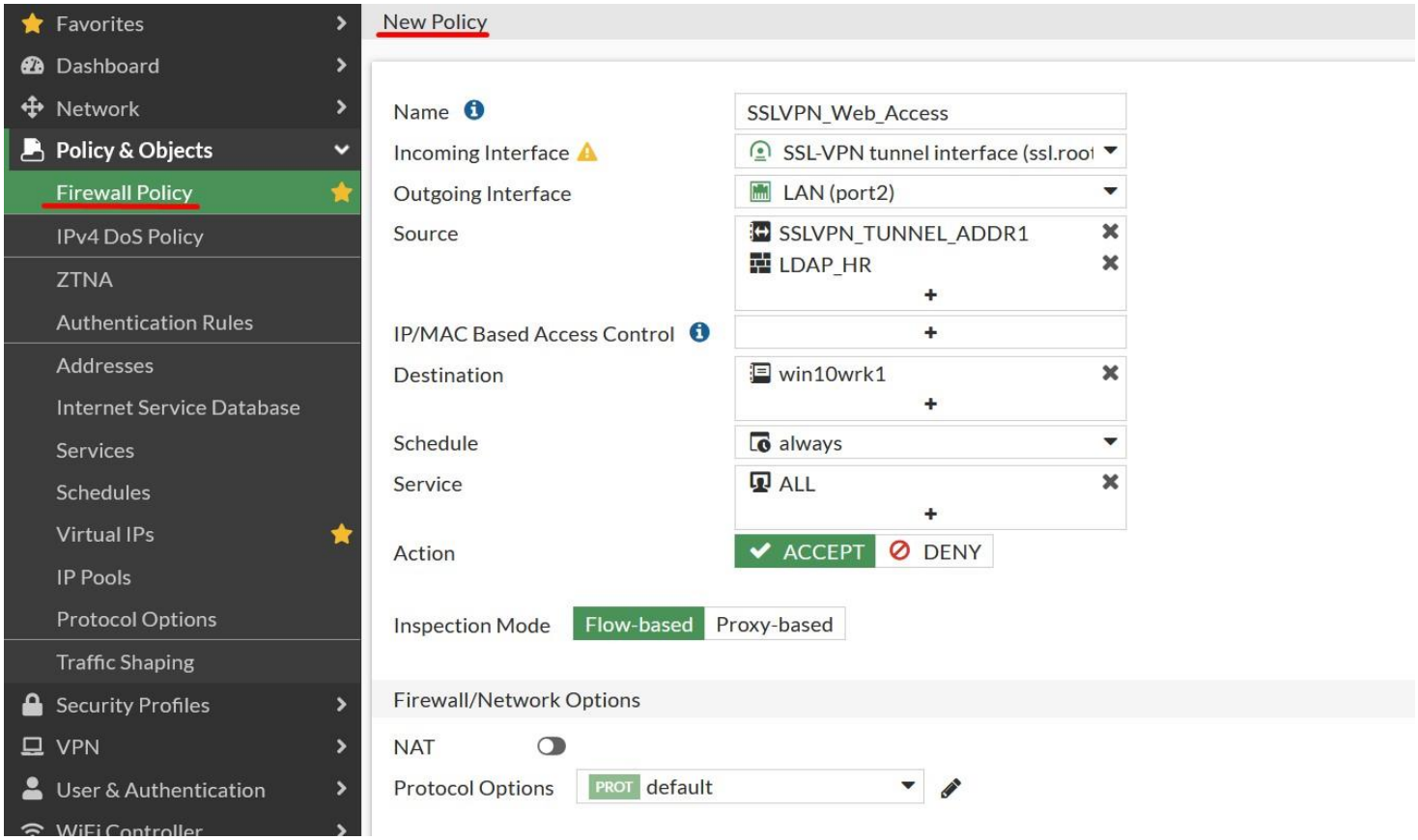


Since we have already set the settings for SSLVPN, we will immediately move on to Authentication/Portal mapping and creating a policy.

We redirect our new group to the WEB portal that we have configured.

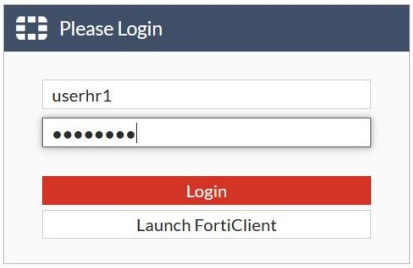


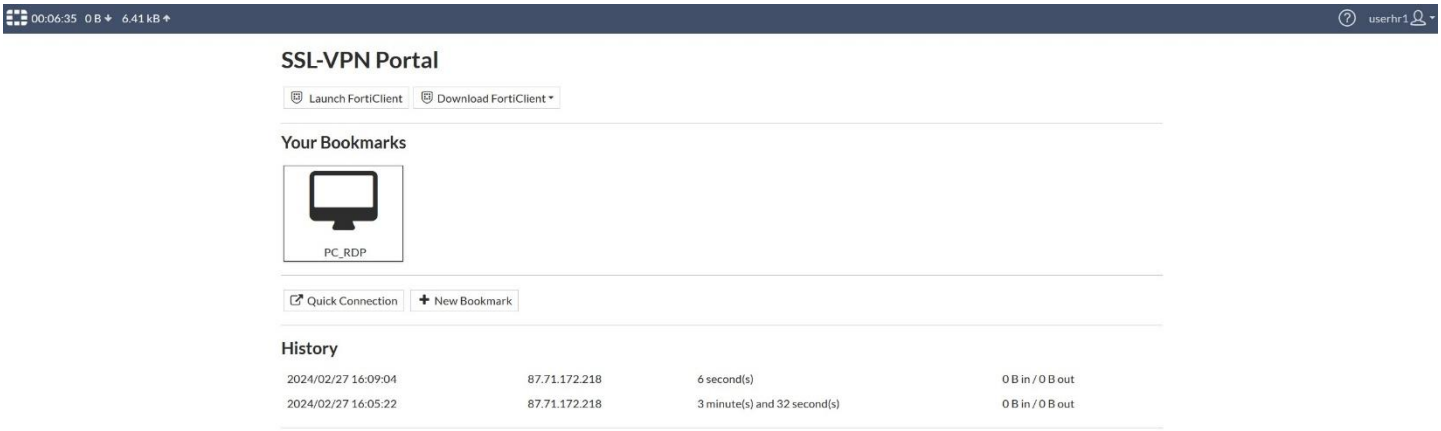
We create a new policy, the incoming interface will be the same SSLVPN and the traffic that will go to our local network, to the PC, we do not need the NAT service since all addresses are already designated in the settings

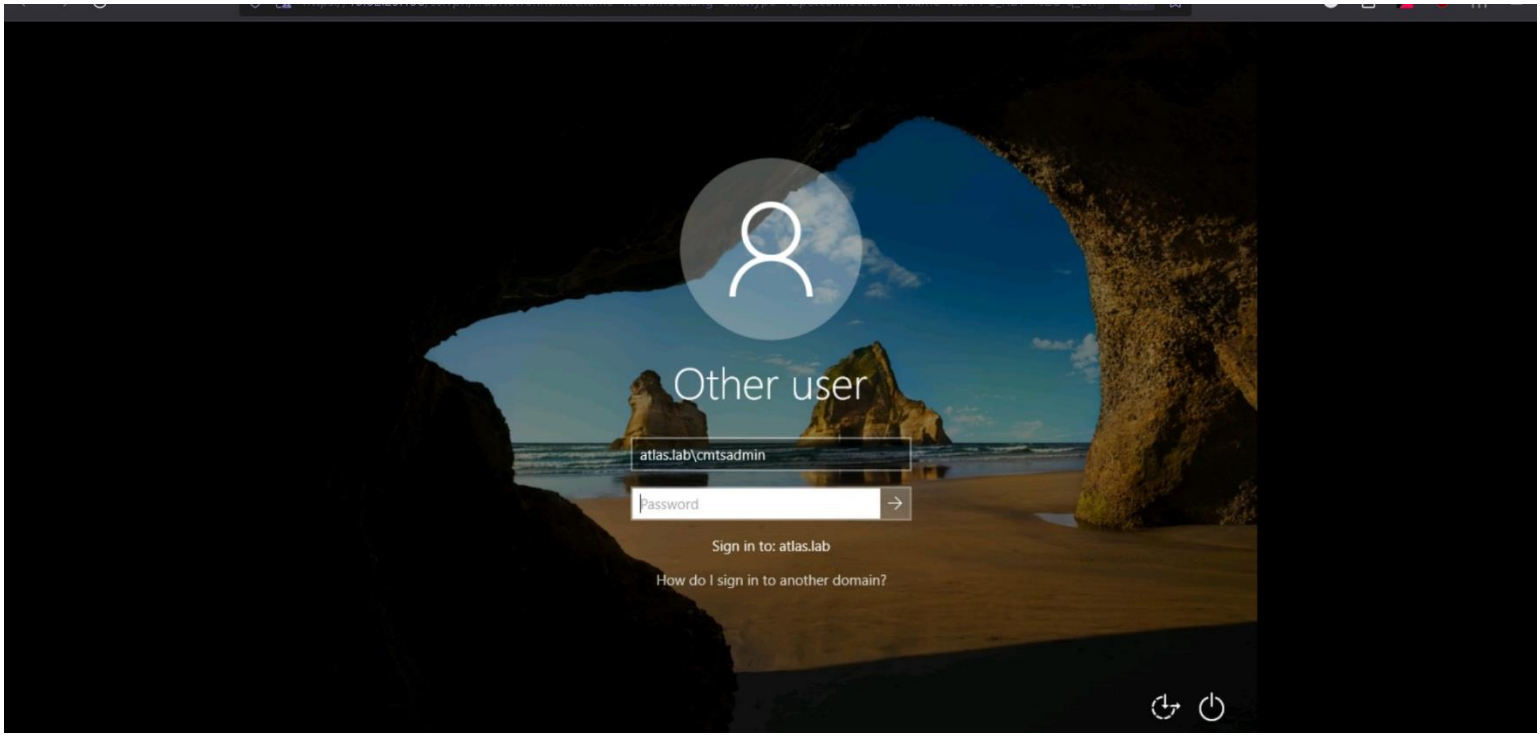


Now let's check it!

We log in as an HP user, and we can see that we were successfully able to log into the remote computer through a web browser. And we entered in with port 443, and on input port 1 the address of which is FortiGate







Virtual IP

- VIP must be created that will allow users to reach the company portal.

1. IIS must be installed in the envario environment on the DC server

2. The VIP searcher must make sure that the article is accessible from the outside

What is VIP in FortiGate?

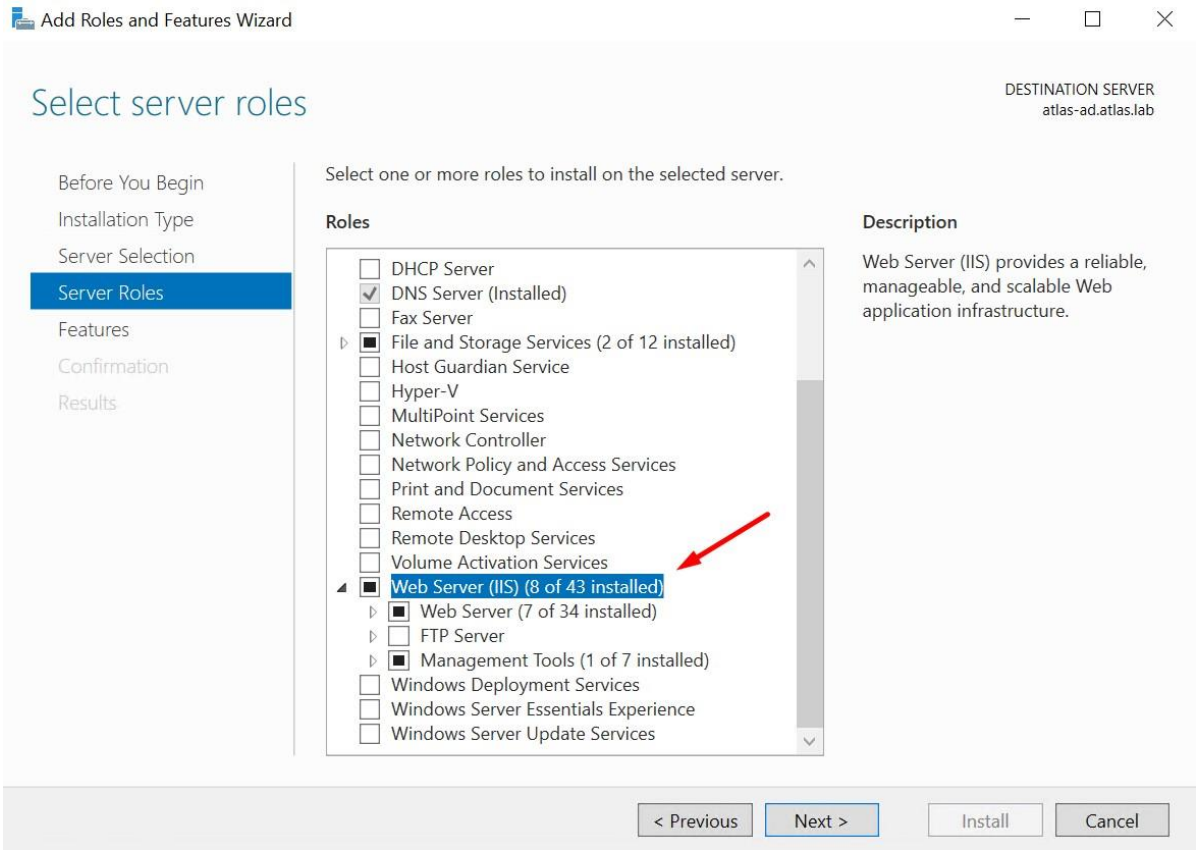
VIP stands for Virtual IP. It's a feature that allows mapping multiple public IP addresses to private IP addresses on your network. This enables services running on internal servers, such as ***web servers*** or email servers, to be accessible from the internet using different public IP addresses.

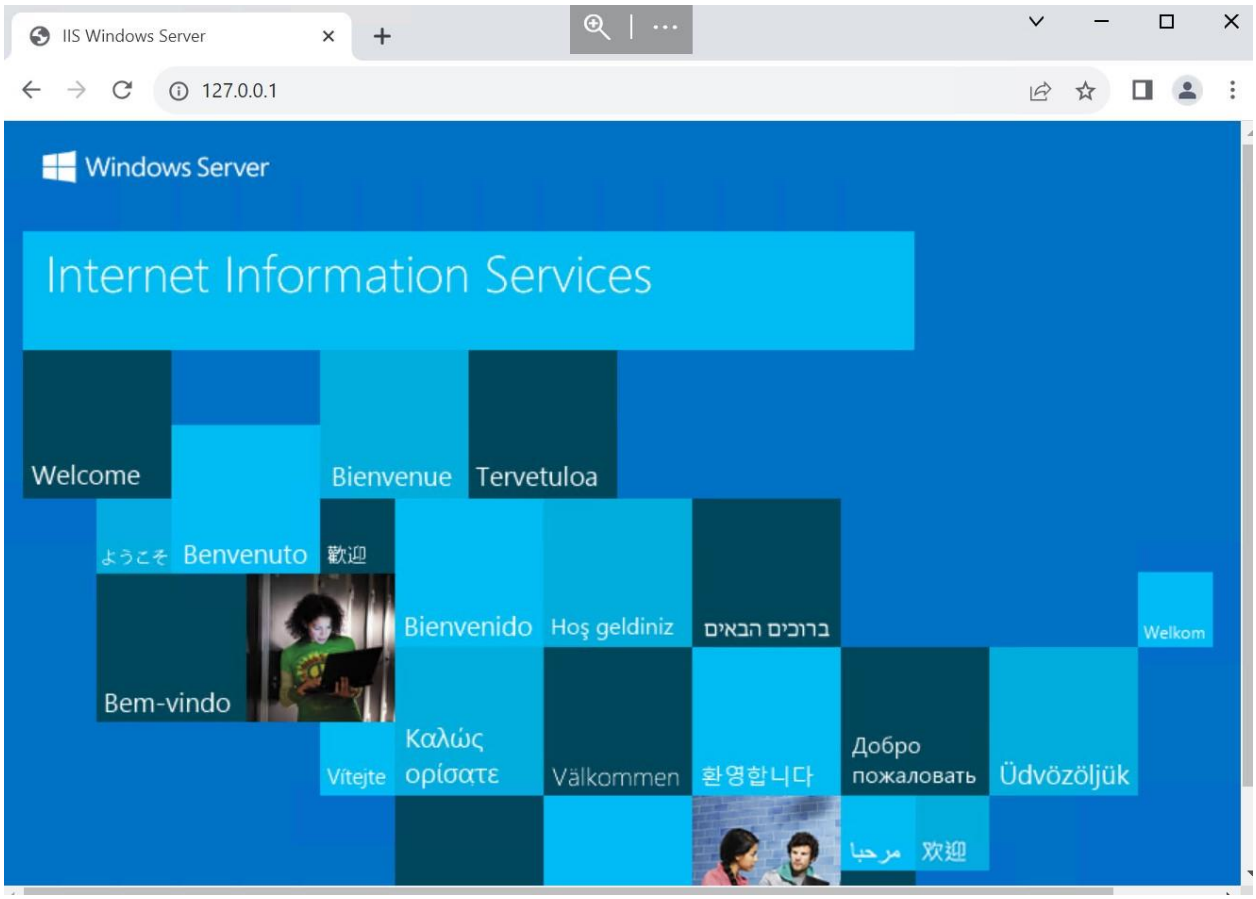
VIP enhances network security and flexibility by enabling traffic redirection and load balancing, all while keeping internal network details hidden from external users.

In a real production environment, we would use a pool of addresses issued by the Internet provider for the company, specifically for websites, and so on. In our simulation we will use PORT 1 (WAN) i.e. the input address of FortiGate

First, let's create the Website in the Active Directory itself and check if it works by going to the address "Loopback 127.0.0.1"

Install the Website Role on our Atlas server and check if it works.



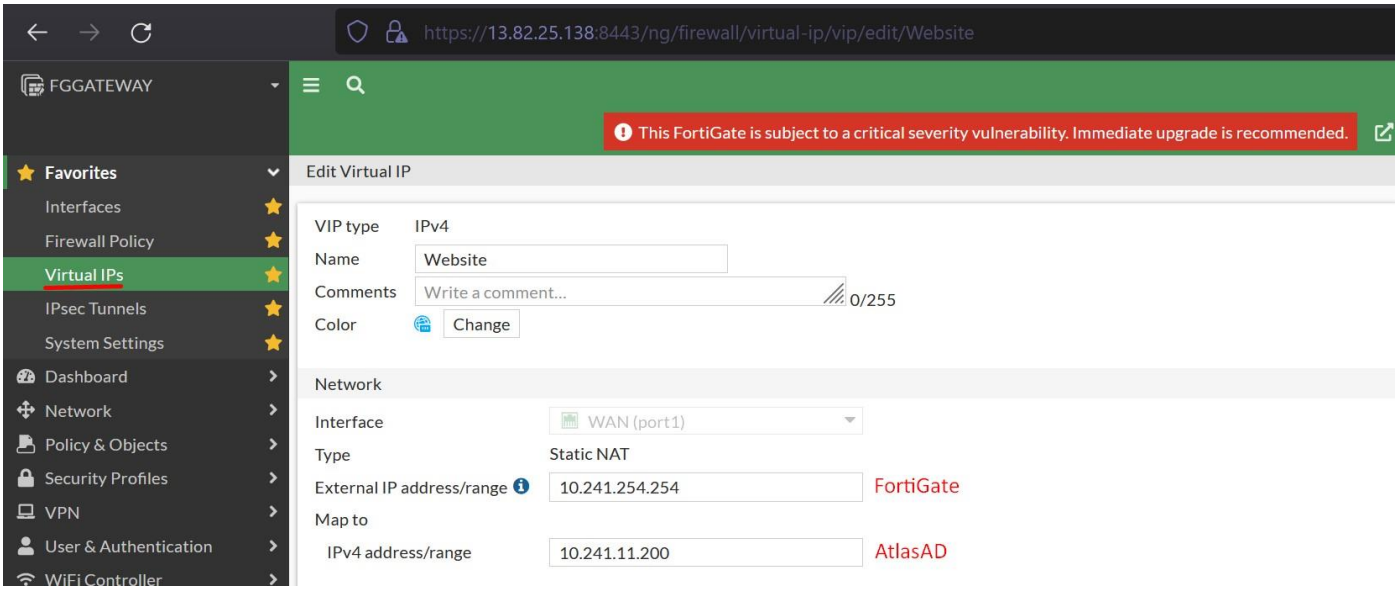


What is Loopback address?

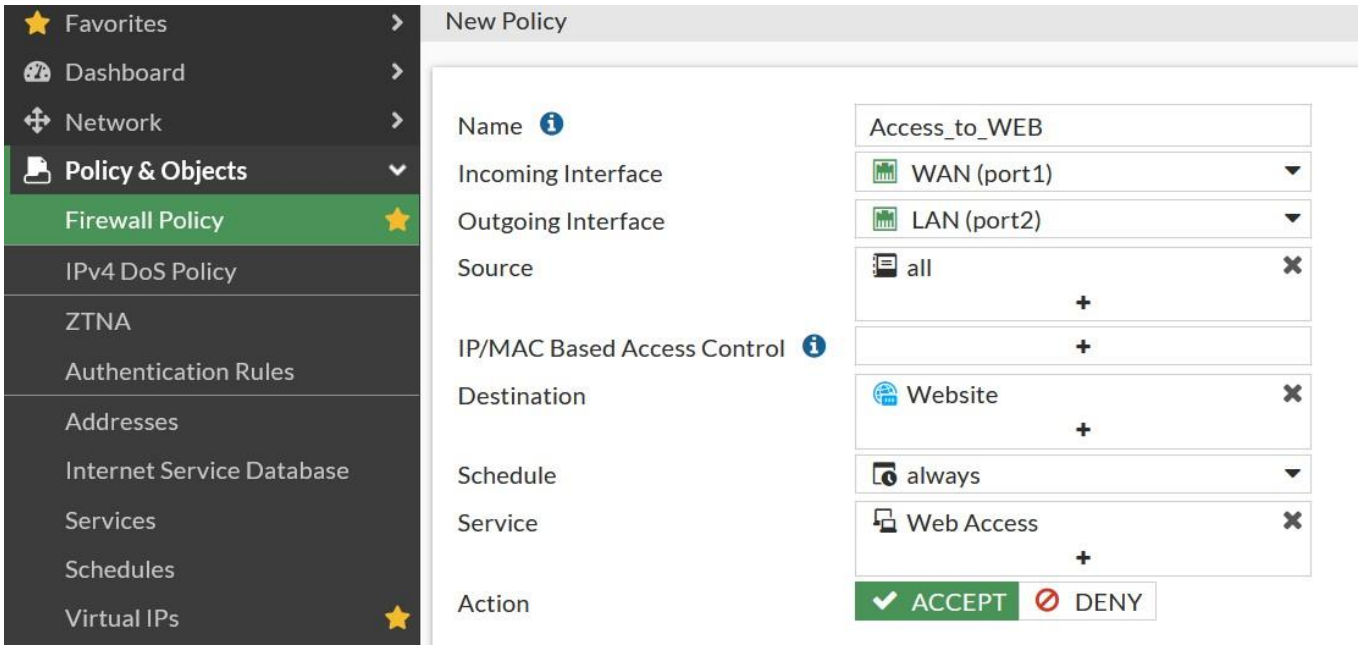
A loopback address, like `127.0.0.1` for IPv4 or `::1` for IPv6, is a special IP address that allows a device to communicate with itself.

Data sent to this address is looped back internally without going through a physical network, often used for testing and local communication within a device.

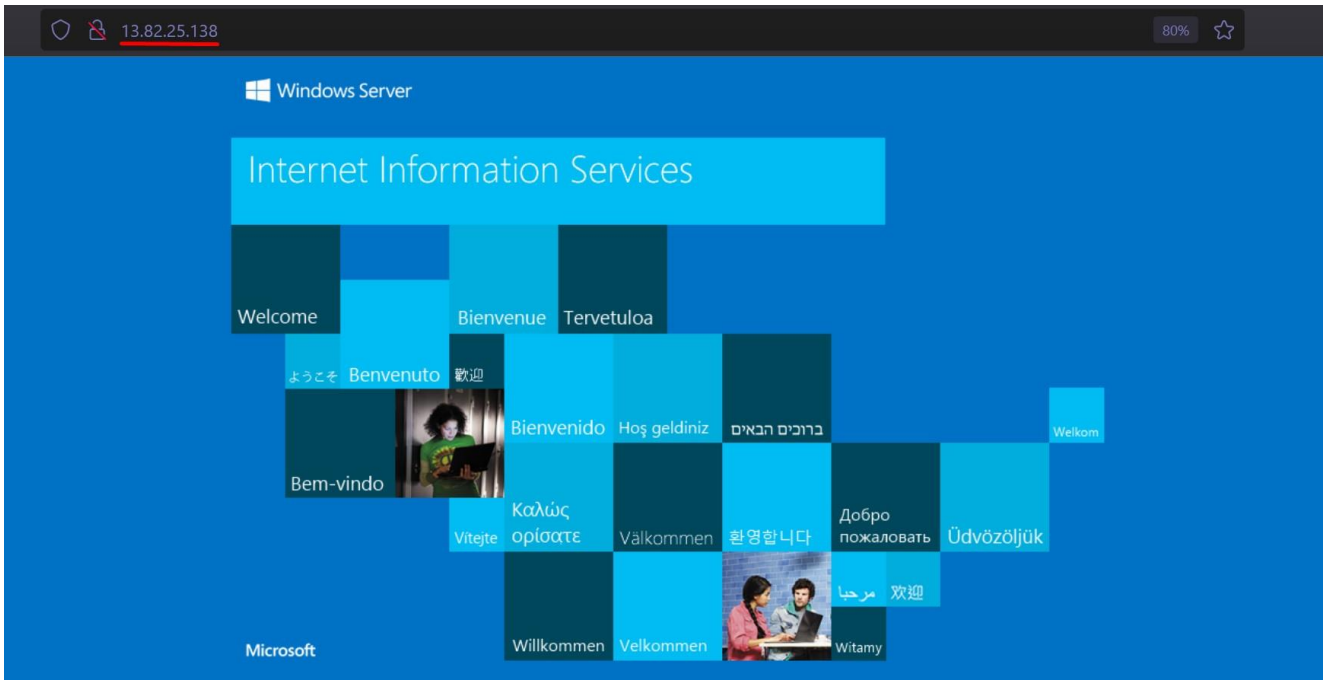
Now we need to create a new virtual address for our website. The interface will be address of FortiGate and the address of the atlas server where the traffic will be redirected.



And as we already know, without a policy nothing will work for us, so let's configure it, the incoming port will be PORT 1 (WAN) and the traffic will go to the local network, the destination is website and the web access service which contains Internet protocols (HTTP , HTTPS, DNS)



And how can we notice the website/VIP is working!



IPsec

- IPsec must be created with a classmate.

1. The Tel Aviv side is allowed to arrive by RDP on the NYC side only
2. The NYC side is only allowed to reach TLV by pinging.

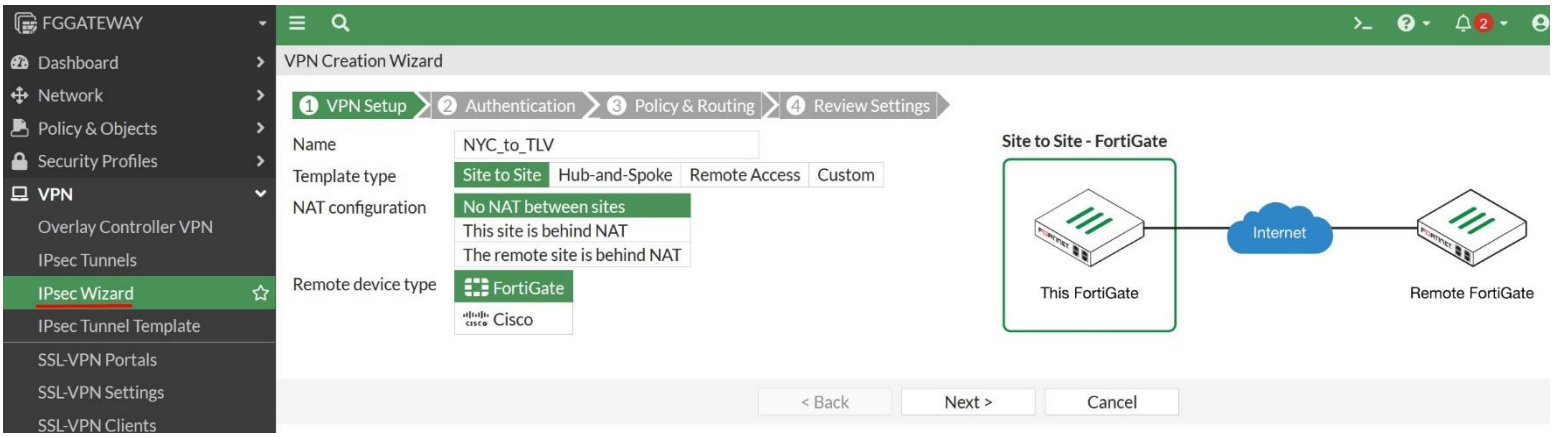
What is IPsec?

IPSec (Internet Protocol Security) is a protocol suite used for secure communication over IP networks. It provides authentication, encryption, and integrity verification for data transmitted between network devices.

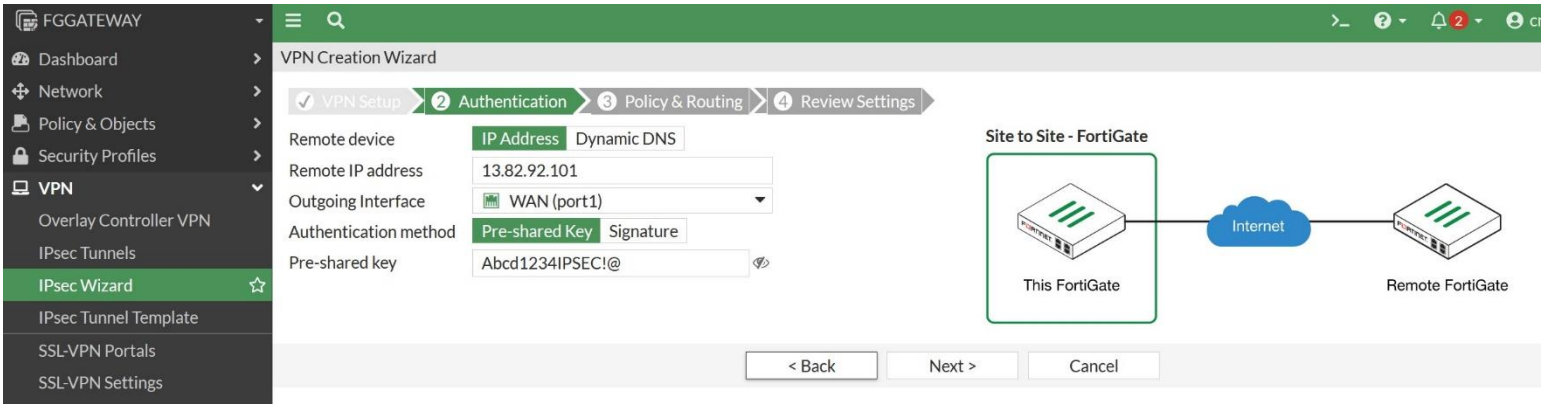
IPSec in FortiGate is commonly used to establish secure VPN tunnels between different networks, ensuring confidentiality and integrity of data transmitted over the internet or other untrusted networks.

In our case, we will connect two cities, I am from New York to create an IPSEC with Tel Aviv, let's start the installation.

First, we go to the IPsec tab and create a new tunnel, give it a name, the connection will be between two FortiGate's



We designate the Tel Aviv IP address as 13.82.92.101 (WAN of Tel Aviv) and create a symmetric key between us and the outgoing interface will be PORT 1 - which goes out to the public network from my FG.

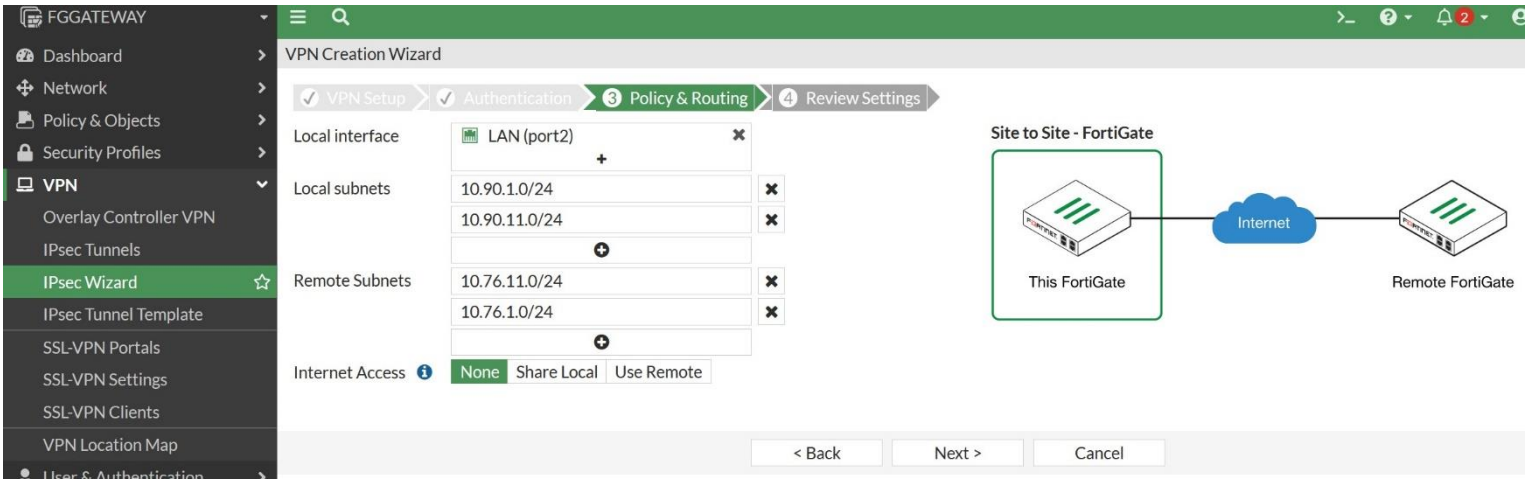


Next step,

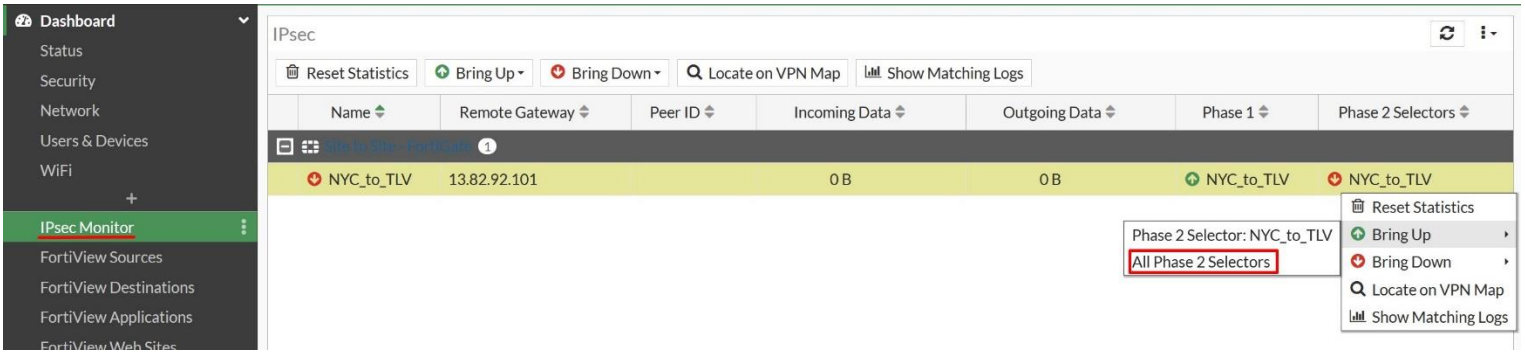
We will write our local networks in which our PCs and Atlas Server are located

New York - 10.90.1.0/24, 10.90.11.0/24

Tel Aviv - 10.74.1.0/24, 10.74.11.0/24

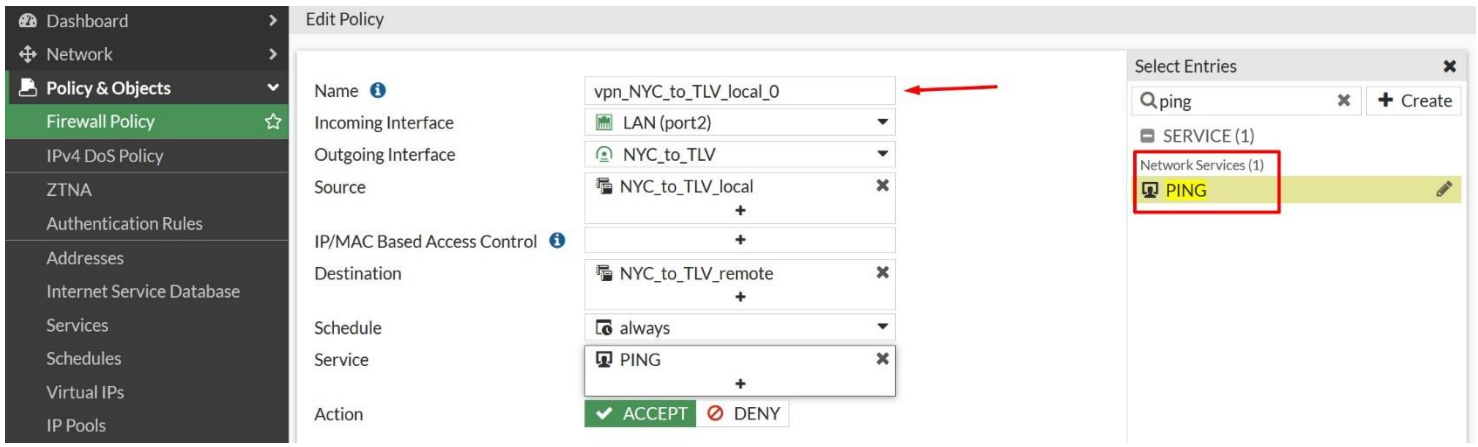


My friend did the same steps only in reverse in his laboratory, now all that remains is to activate the second phase and after that our connection will be established.

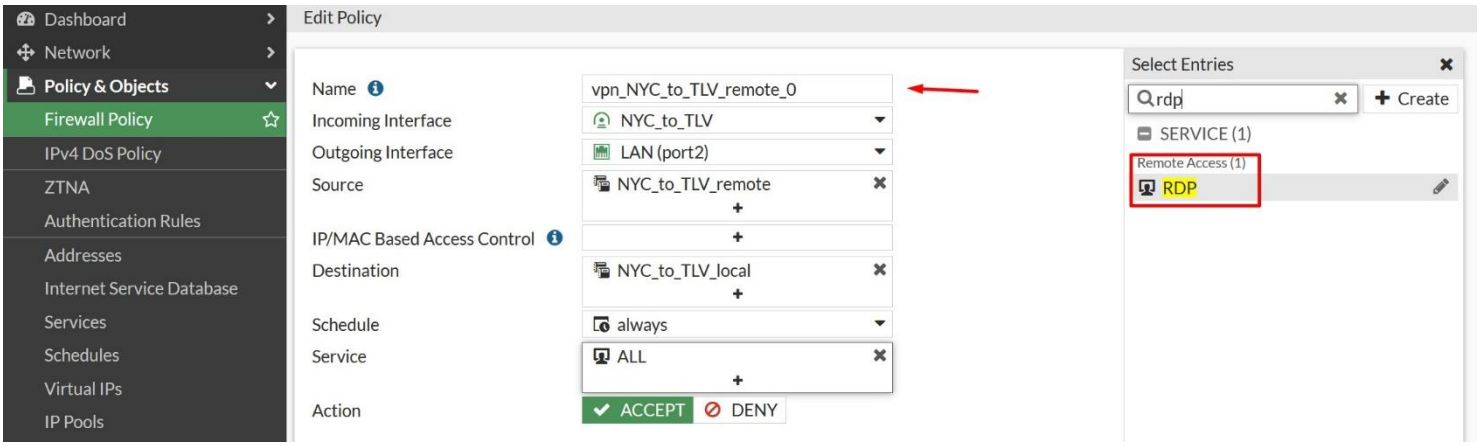


Now, according to the assignment, we need to set up a policy so that only New York can ping to Tel Aviv and Tel Aviv can connect via RDP to my local machines, since during the creation of the IPsec tunnel, automatic policies were created, we enter them (Policy) and change the services to we need.

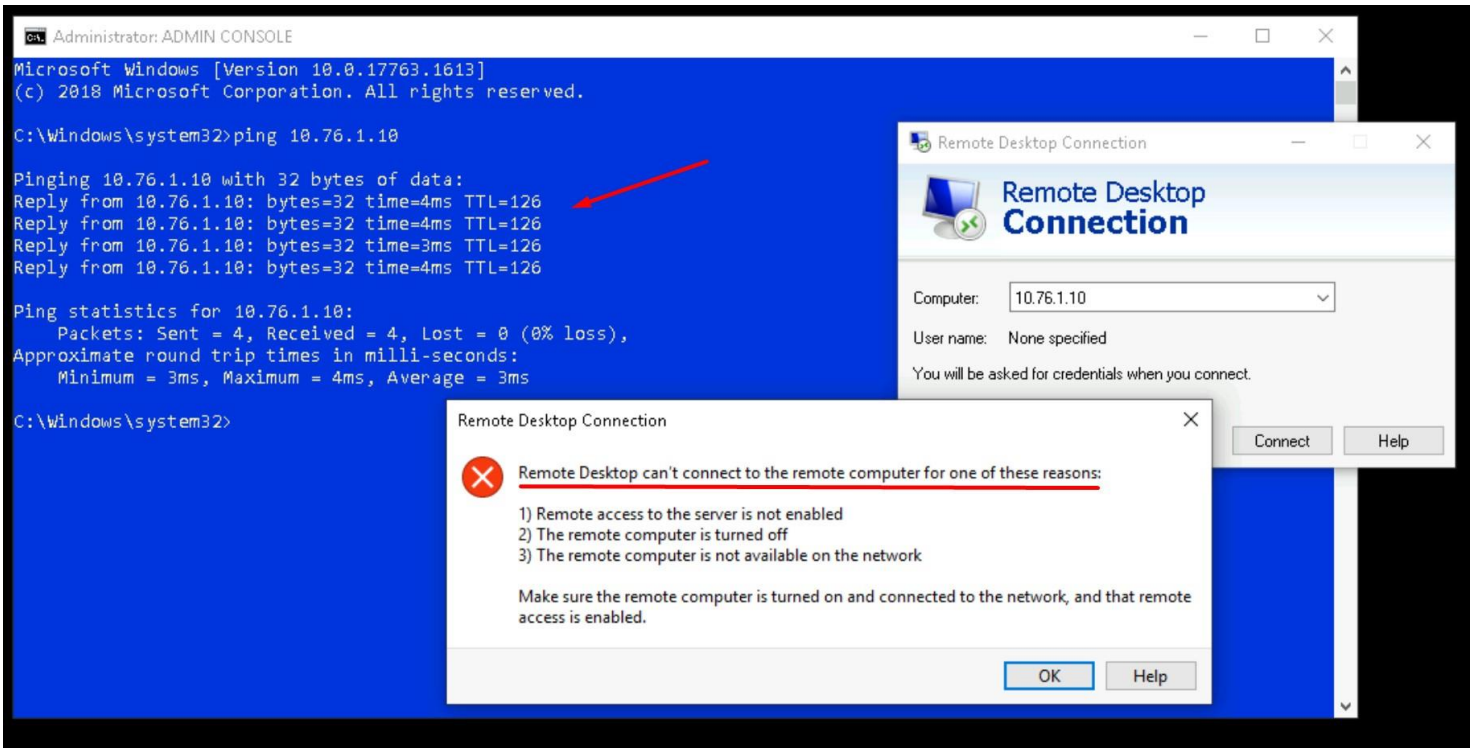
NYC to TLV (Just PING)



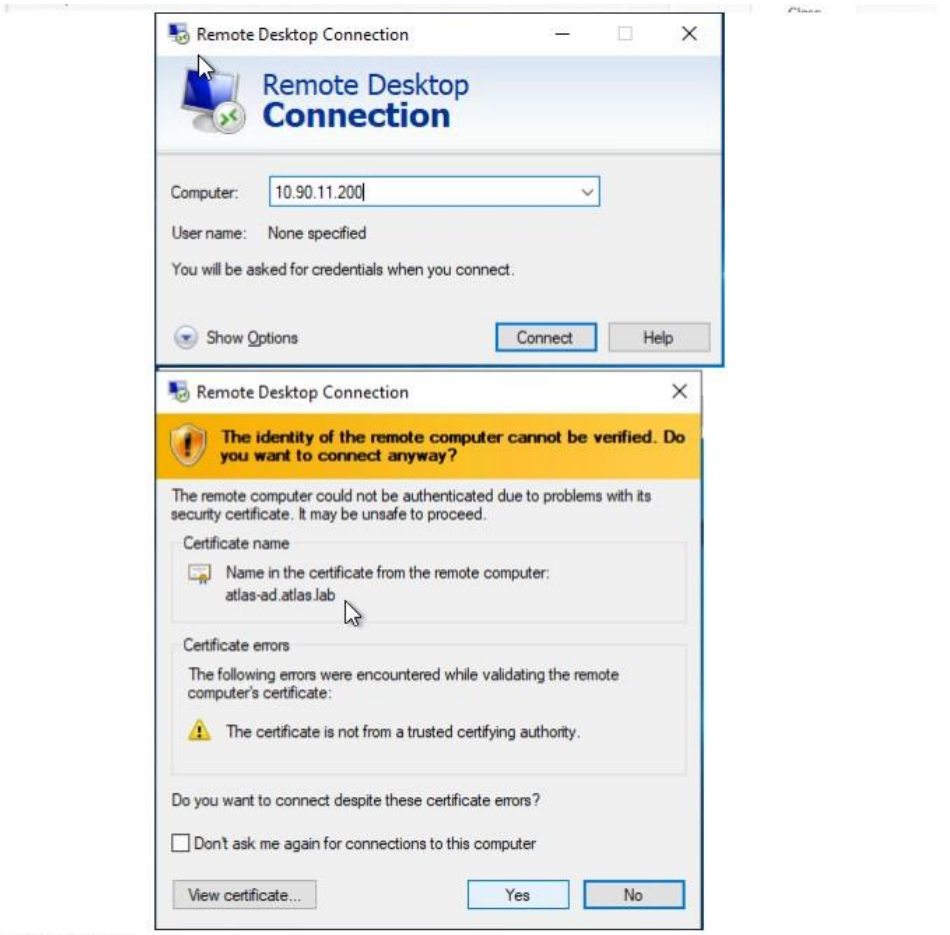
TLV to NYC (Just RDP)

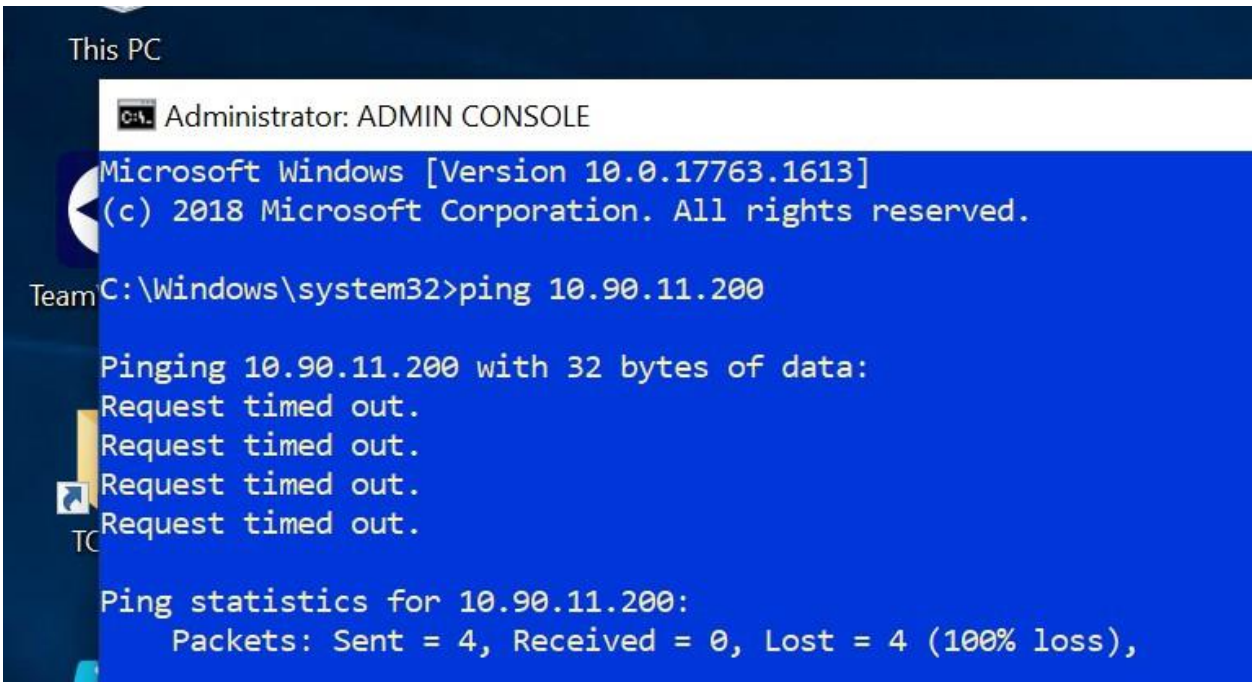


After checking on both sides, we can make sure that the policies and the connection are working.



screenshots of my classmate





SSL/TLS Inspection

- Create a new inspection profile called Office_To_Internet_Inspection

1. The profile must be configured in Full SSL Inspection mode

2. In a few words, explain what is needed and why it is used

in inspection

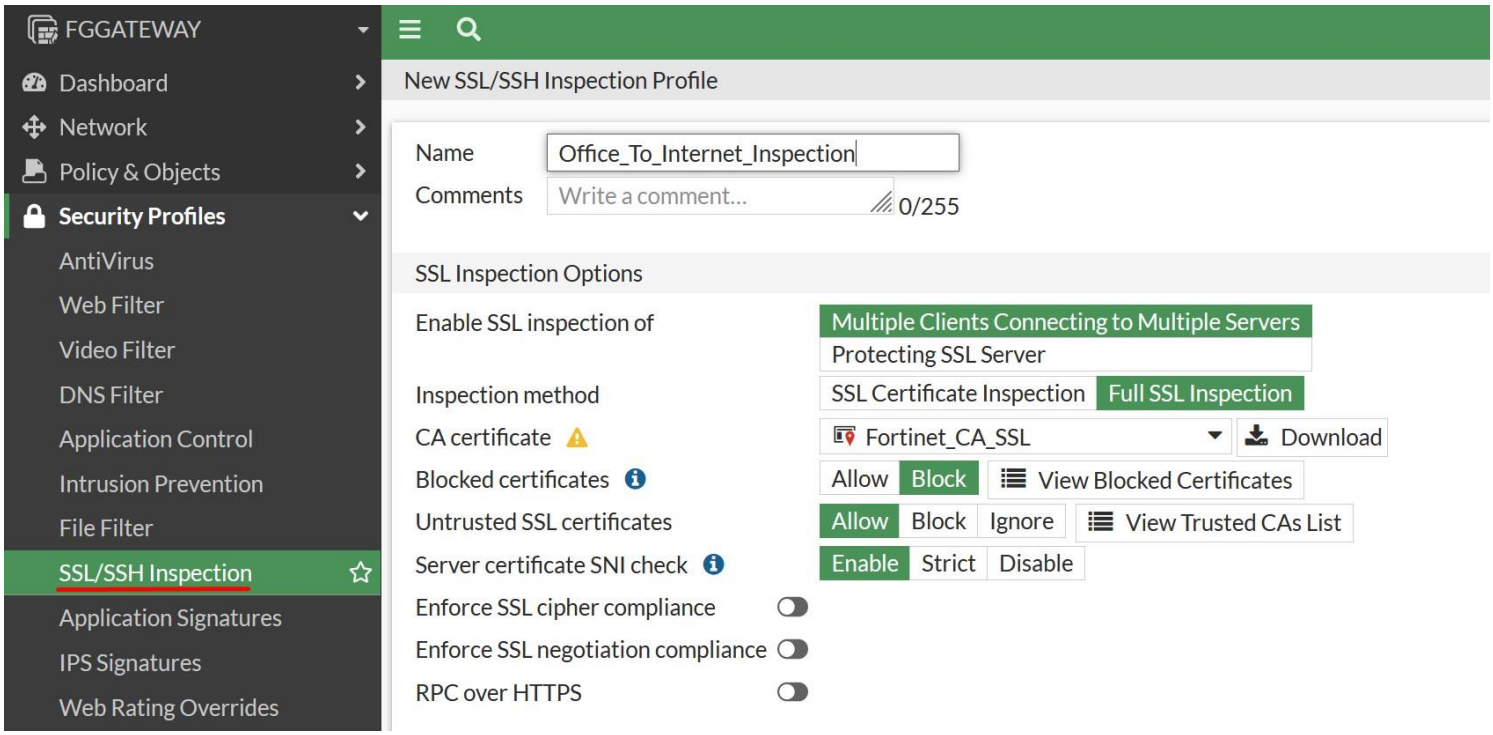
What is SSL/TLS Inspection?

SSL/TLS Inspection is a feature that allows the firewall to decrypt and inspect encrypted SSL/TLS traffic passing through it. This process involves intercepting encrypted traffic, decrypting it, inspecting the decrypted content for threats such as malware or policy violations, and then re-encrypting the traffic before sending it to its destination.

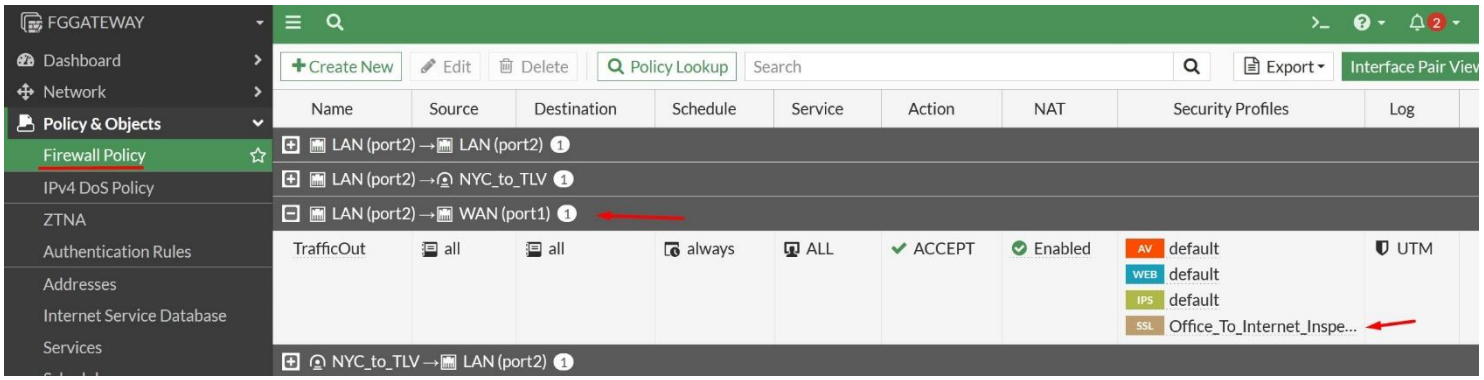
SSL/TLS Inspection helps enhance security by providing visibility into encrypted traffic, allowing organizations to enforce security policies effectively and detect potential threats hidden within encrypted communications.

Many other network security appliances and solutions also offer SSL/TLS Inspection capabilities. These include products from vendors such as Palo Alto Networks, Cisco, Check Point, SonicWall, and others.

We'll set it up so that everyone can access many services, and we'll also choose a full inspection method so that it opens and checks everything, every packet at once.



And we will choose this inspection at the exit from the FortiGate, at the Traffic out port.



Web-Filter

- Create a Web-Filter profile named Office_Web_Filter

The profile must be set in base “Proxy mode” - explain in a few words what the situation is It?

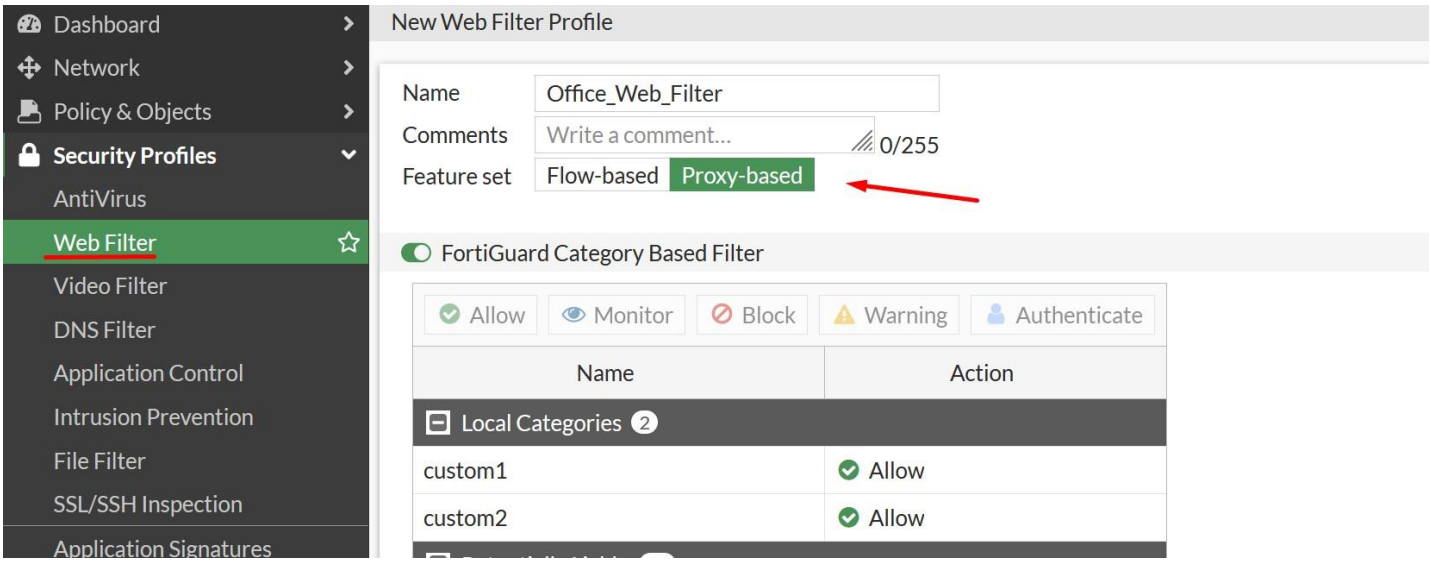
Why is it needed?

The Web Filter feature allows administrators to control and monitor web access based on predefined policies. When operating in "Proxy mode," FortiGate acts as an intermediary between the user and the internet, intercepting and inspecting web traffic in real-time.

The first and main problem is malicious and unknown sites. A web filter filters these sites and blocks user access to them, thereby protecting the organization's users and the organization itself.

"Flow-based" refers to a method of packet processing where network traffic is analyzed and managed based on its flow characteristics, such as source and destination IP addresses, ports, and protocols. Flow-based processing allows for faster packet inspection and decision-making compared to traditional packet-by-packet analysis.

Let's move to the web filter, create a new one and select the proxy base mod.



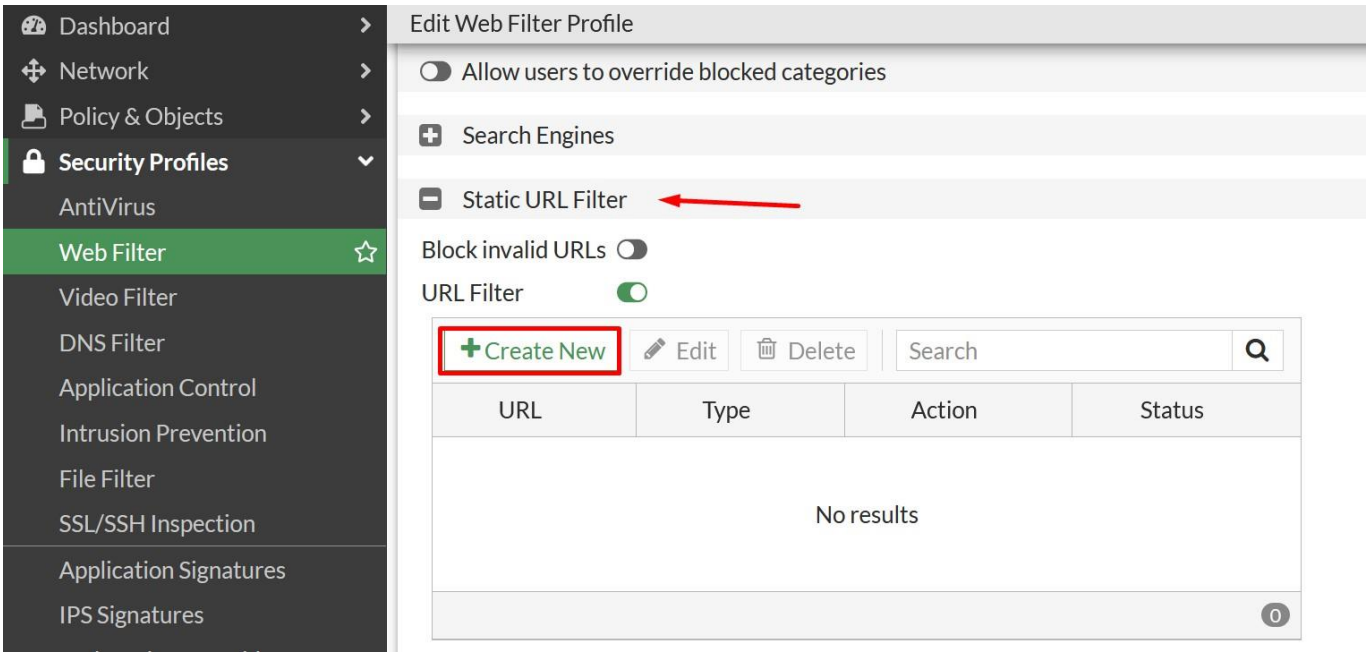
- Access to sites in the job search category must be prevented.

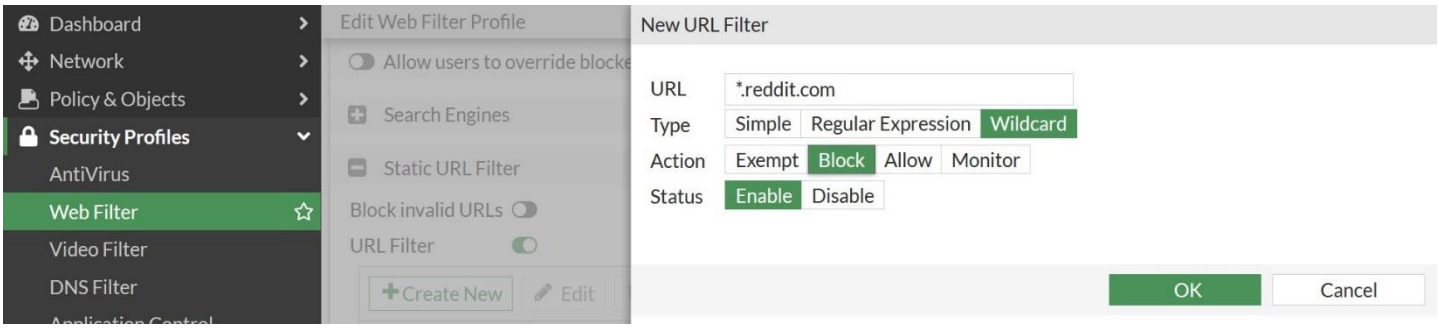
1. Denied access to the site - reddit.com.

2. Make it possible for specific users to access a category of a type shopping and everything else is not. (Identification with a user and password)

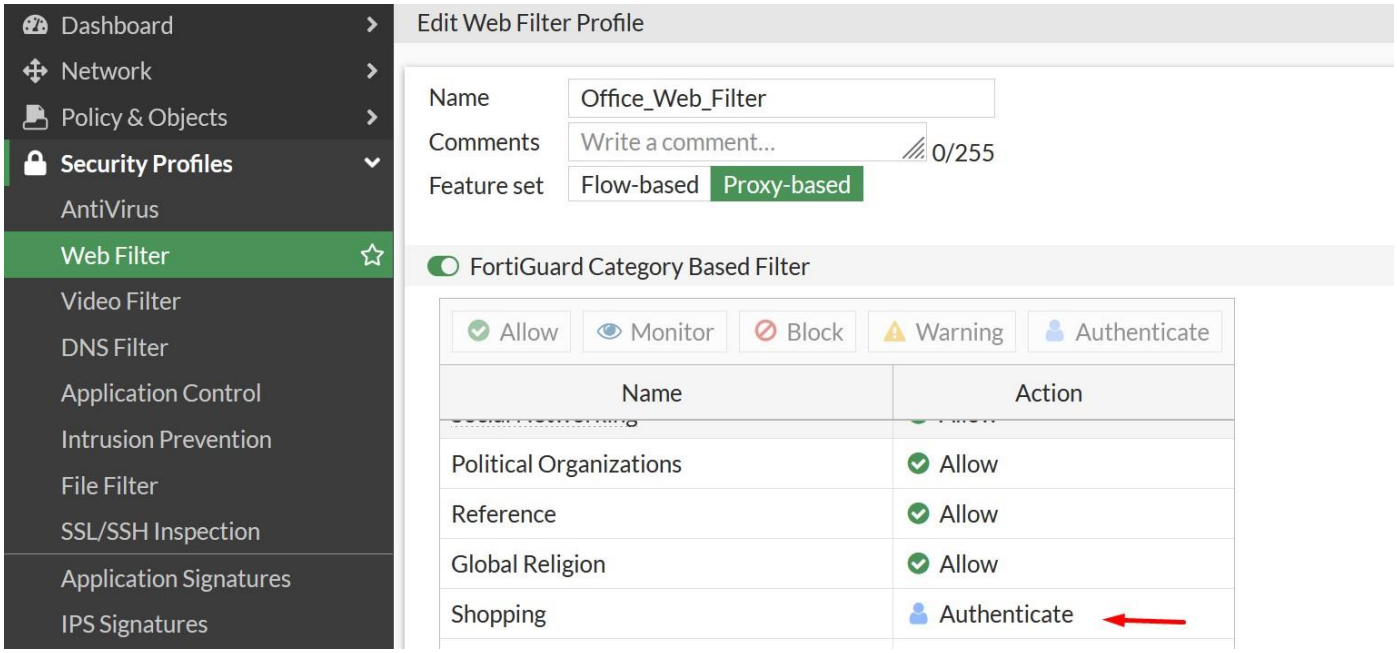
Now let's block a site for example, let's take reddit We will also open access to the "shopping" category for some users and exclude everyone else.

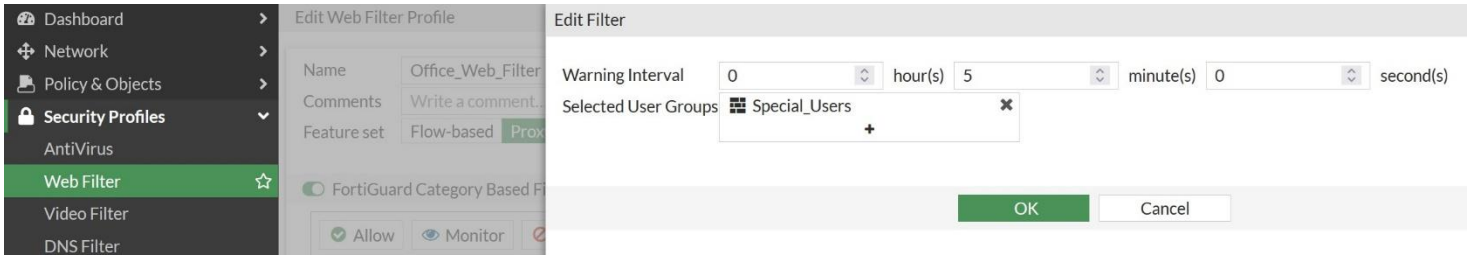
We will go to the same Web Filter, and select a static URL profile and block the reddit site, as well as all its subdomains and records (*).



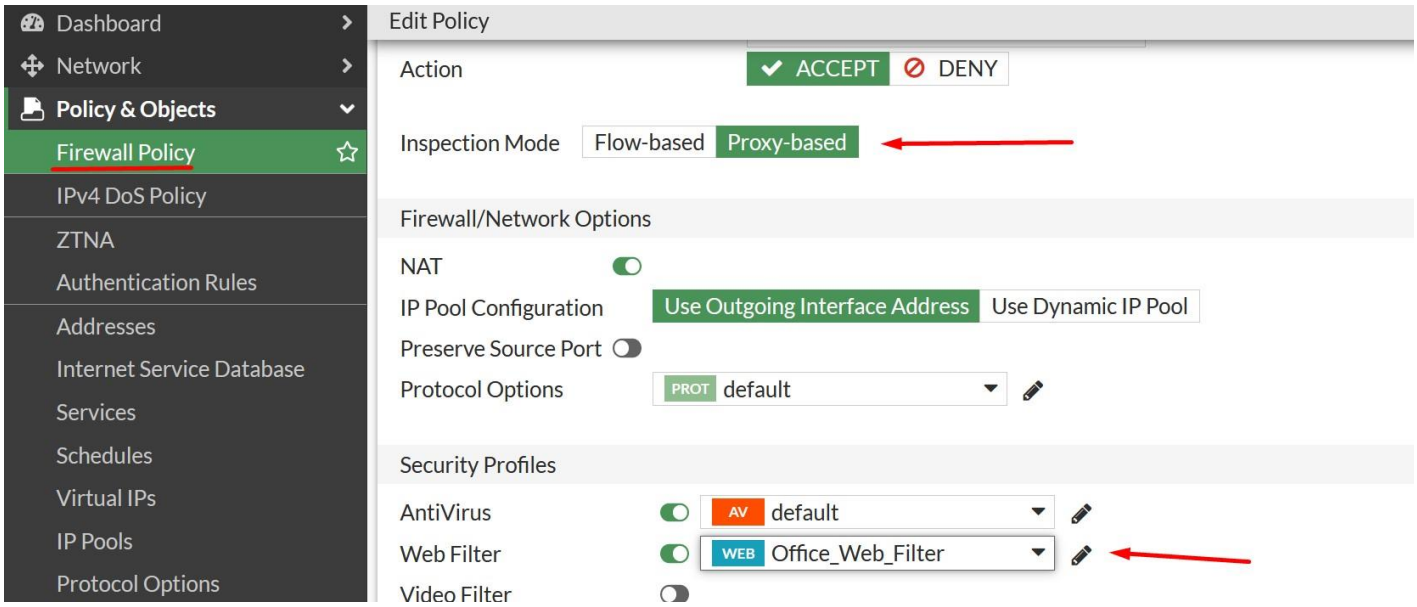


Scroll up and we will select the category of shopping next, I'll set the Action to authorization, then select the group of users that will be included in this number.

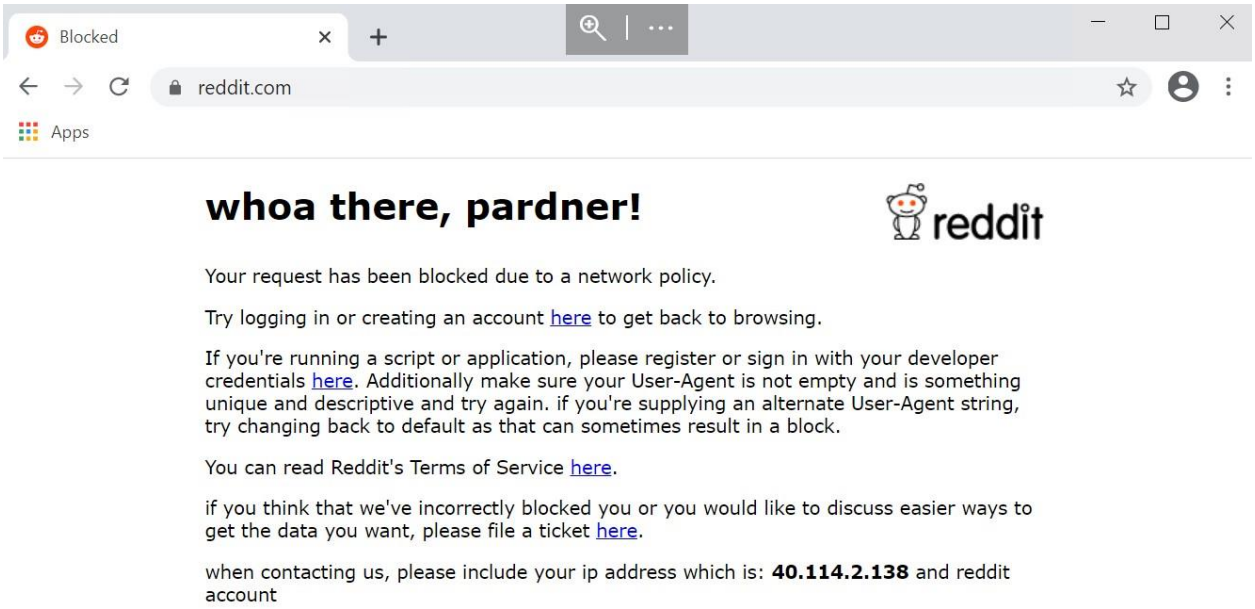


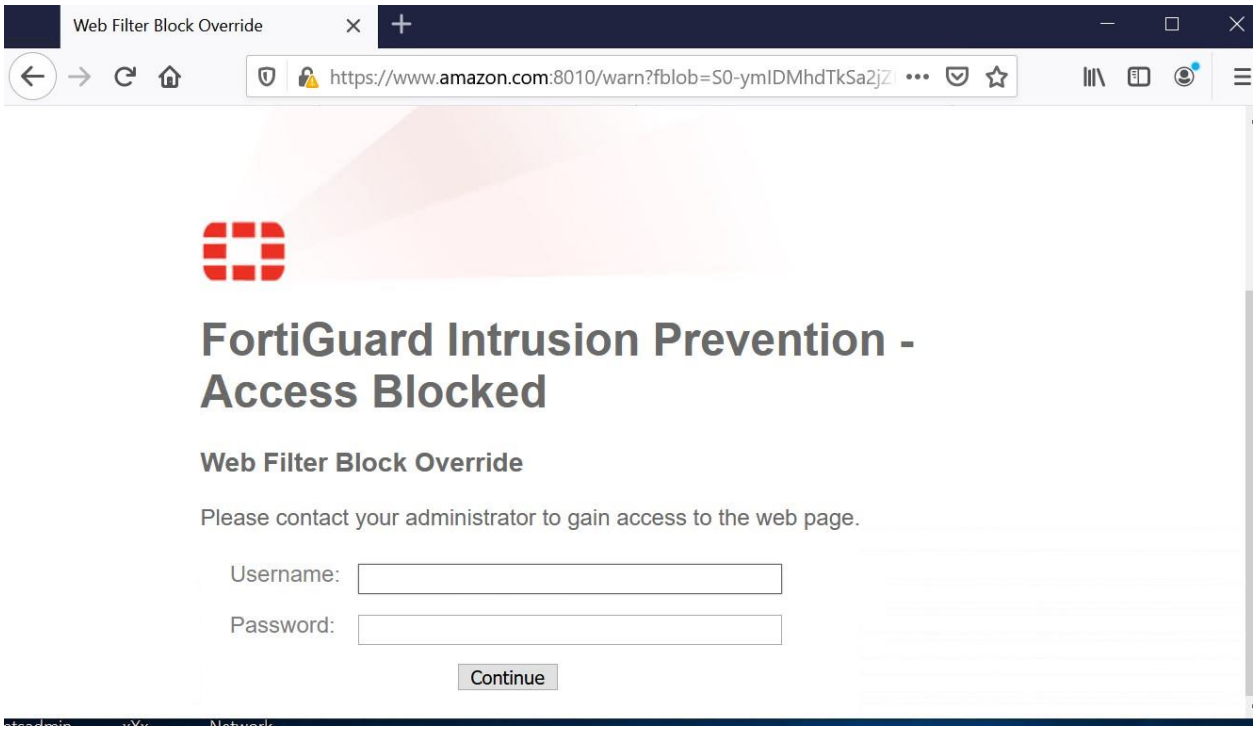


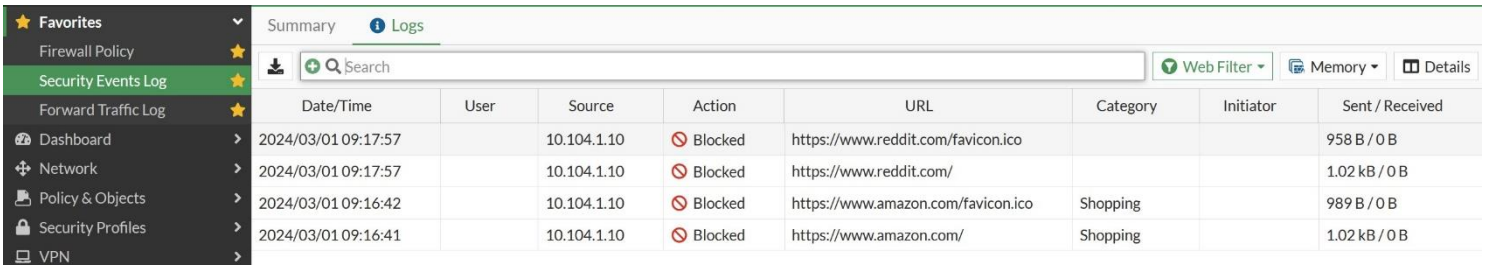
Now we will move to our "traffic out" policy and select the new web filter that we just configured.



And how can we see that all filters are configured, the shopping category is open by authorization, and reddit is also blocked for everyone.







DNS-Filter

- Create a DNS-Filter profile named Office_DNS_Filter

1. Activate a block for C&C type sites and domains
2. Block a specific domain (Domain Filter)

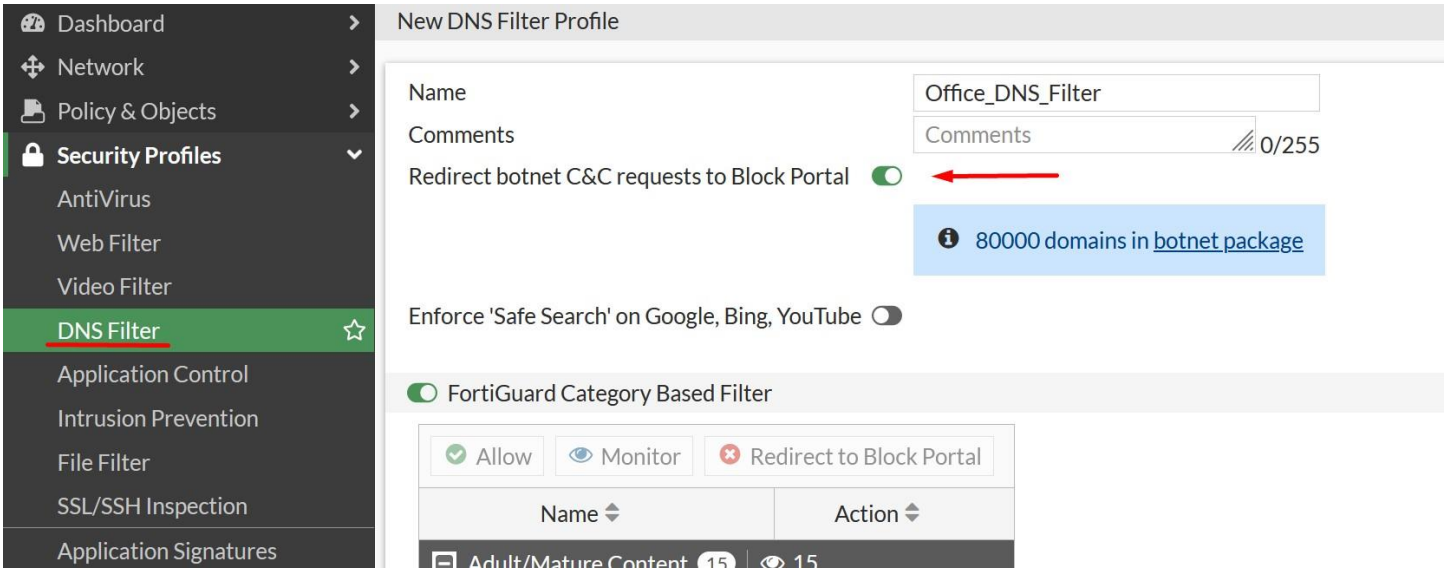
What is DNS filter?

DNS is a very common way to attack and redirect users to visit malicious websites or domains.

Attackers often use different fully qualified domain names to host malicious websites or fishing web sites, and DNS filter will help us with it.

A DNS filter in FortiGate is a feature that allows administrators to control and monitor DNS (Domain Name System) requests made by devices on the network. It works by intercepting DNS queries and matching them against predefined policies to determine whether to allow, block, or redirect the requested domain.

Let's create a new filter and enable the mode for blocking and redirecting botnets and C&C requests.



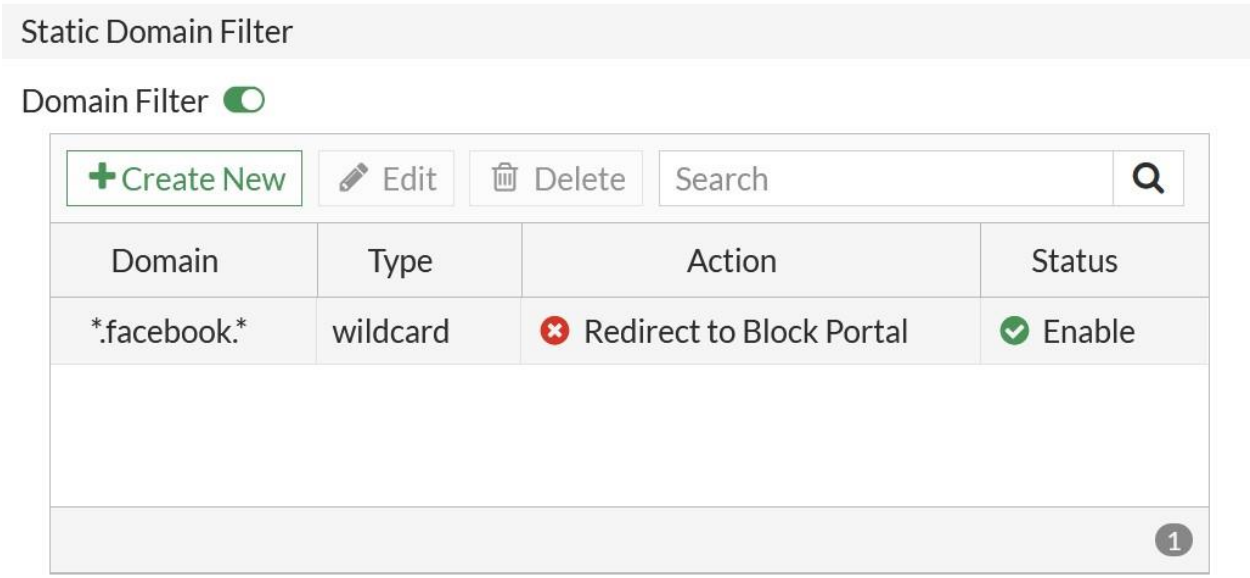
C&C

(Command and Control): Refers to a centralized server used by cybercriminals to remotely control computers, also known as bots, for malicious activities such as launching attacks, stealing data, or spreading malware.

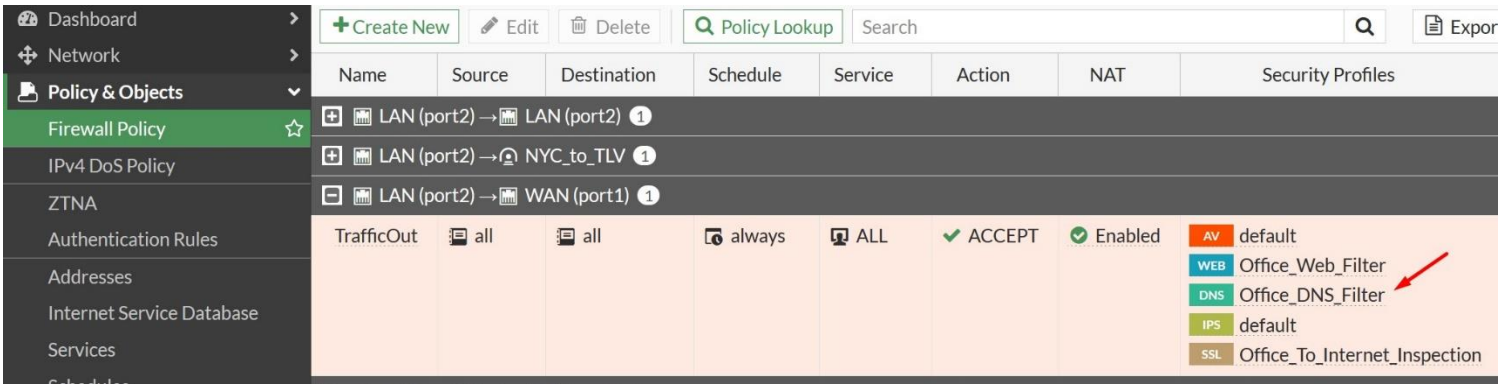
Botnet

A network of compromised computers (bots) that are under the control of a central command and control (C&C) server. Botnets are typically used for coordinated cyberattacks, such as distributed denial-of-service (DDoS) attacks, spamming, data theft, or cryptocurrency mining, leveraging the combined resources of the infected computers.

Now, as an example, let's take the Facebook website and designate it in the DNS filter as a "dangerous site."

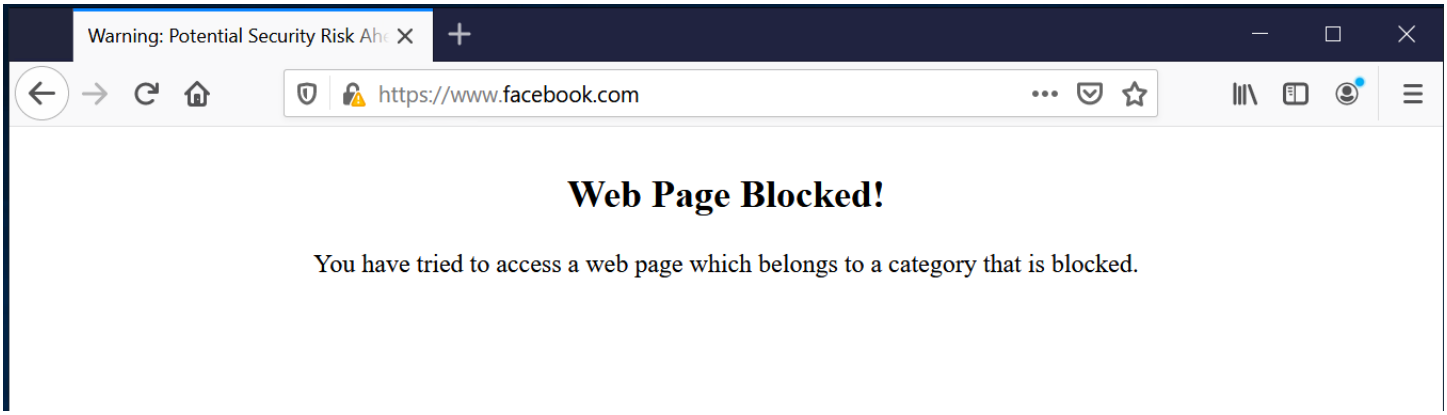


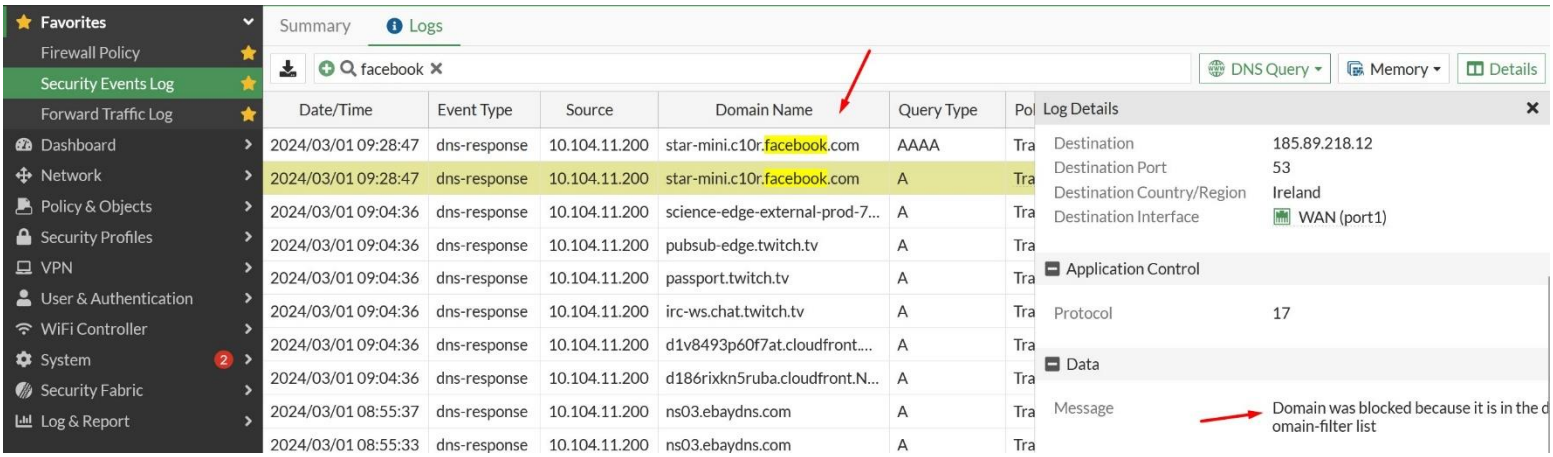
Let's install this filter on the output port and let's check it.



How can we notice that the site is displayed on the client computer as malicious, which is not true, but we gave this site as an example.

These features give us Full control as a network administrator.





Antivirus – Profile

- Create an Office_AV_Profile profile.

1. Set the profile as Flow-Base

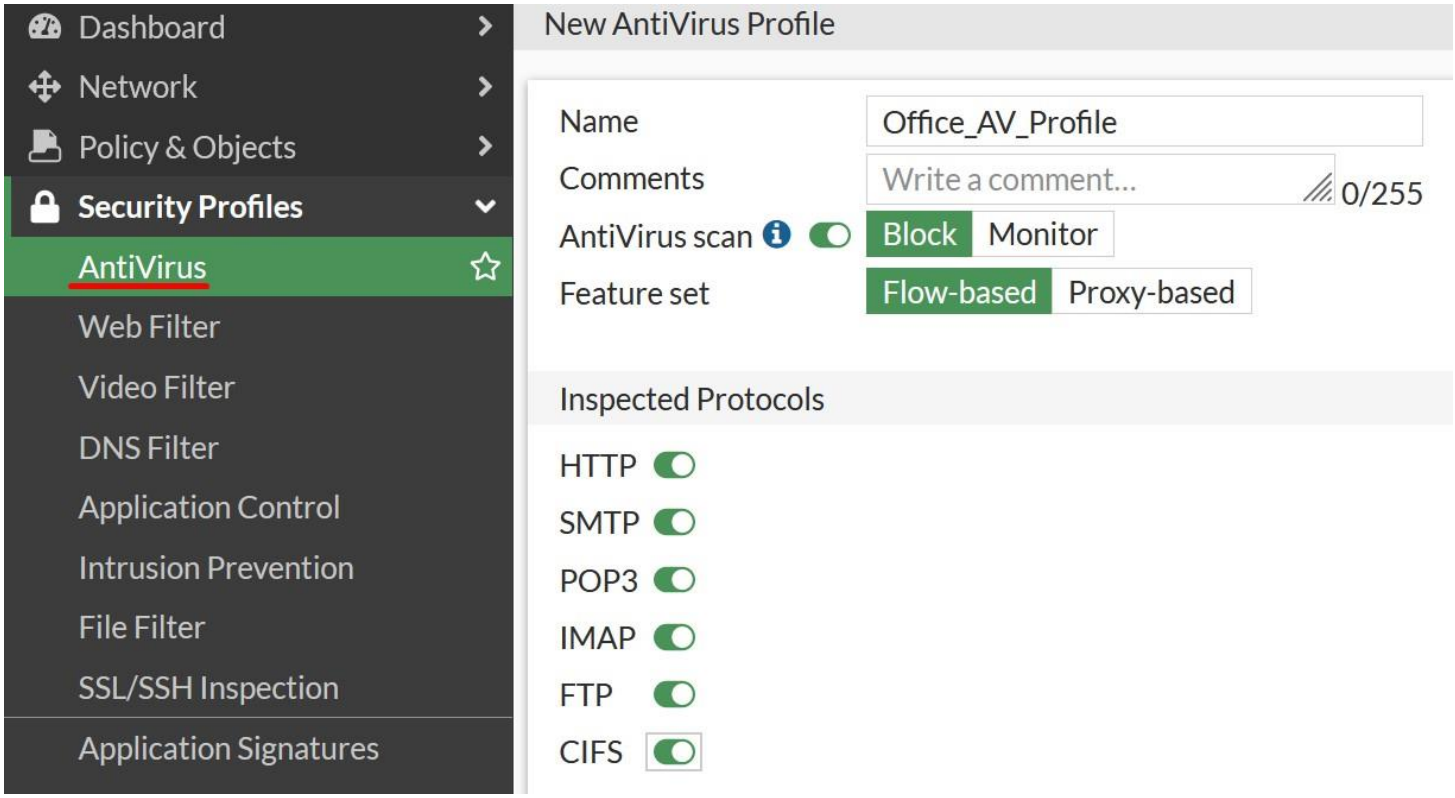
2. Create a situation where files from the attached site are blocked

FortiGate's antivirus works by scanning files using signatures, heuristic analysis, and sandboxing to detect and block known and unknown threats in real-time. Regular updates keep it effective against new malware.

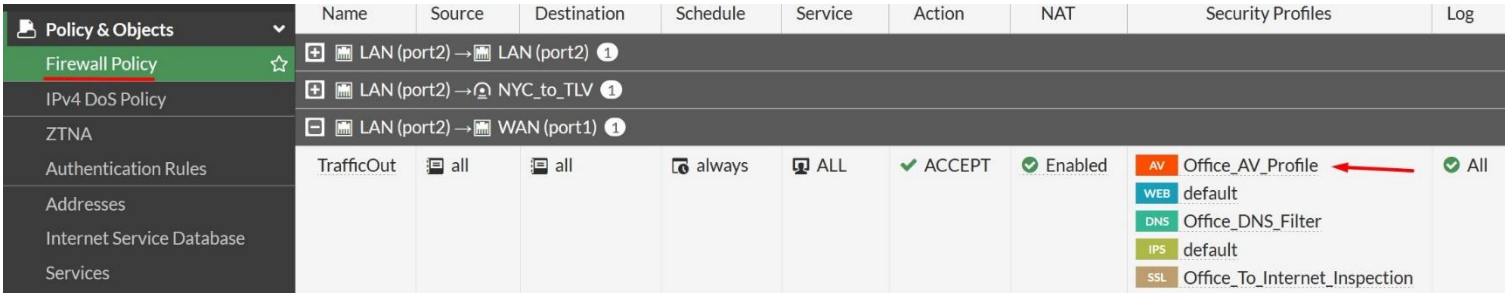
Anti-virus detects viruses by "signature" – a file identified as a virus marked by hash. Every AV company has a database with hundreds of thousands of virus detections and those viruses.

Now we will configure the Anti-Virus and send it to port 1 which goes to WAN, and we will also test it by going to the site via a computer and downloading "test files" with a virus hash.

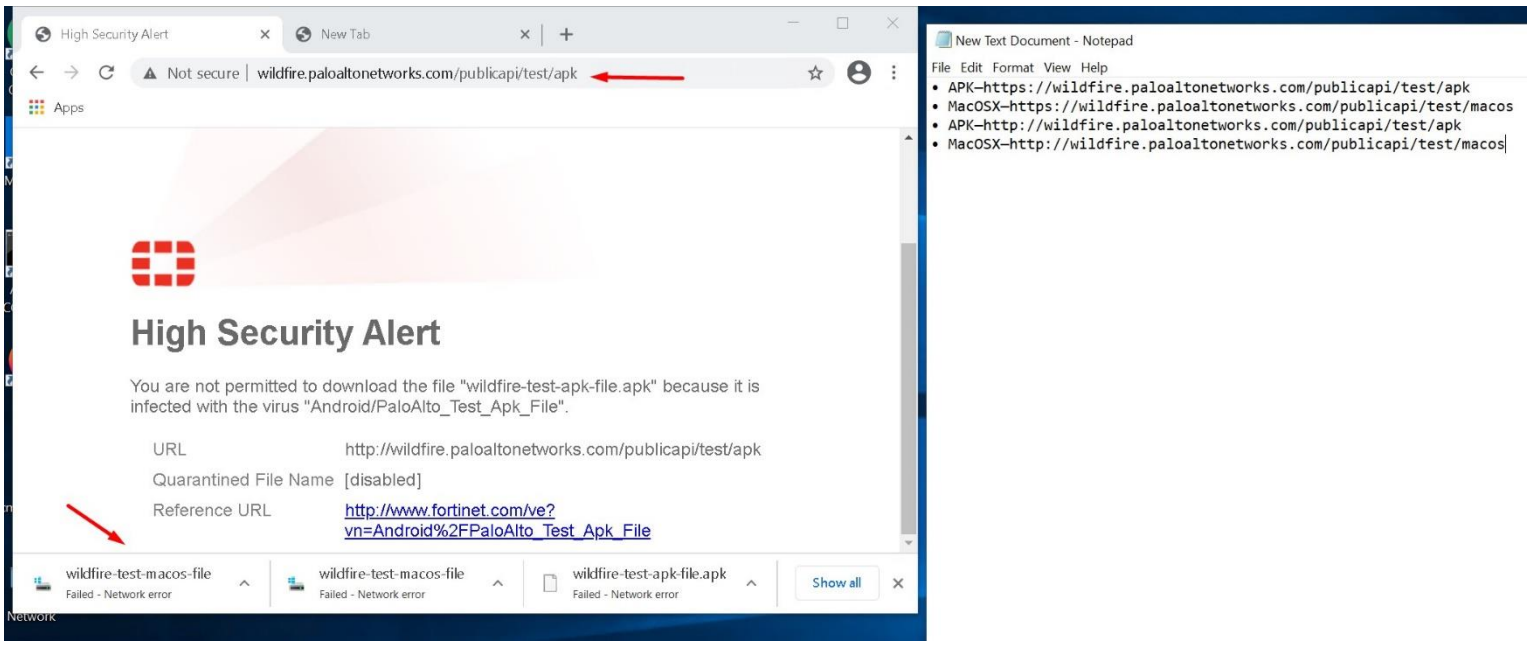
We go to the antivirus profiles and create a new one, set the inspection to all Internet protocols, flowbase and block all viruses



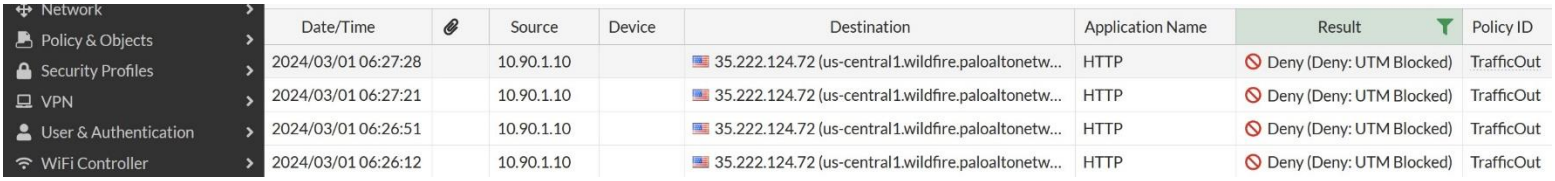
We put this profile on PORT 1



Go to the workstation and check that the antivirus is blocking all potentially malicious links



You can also see this in the logs.



IPS – Profile

- Create a profile called Office_IPS_Profile

1. Write a few words about what IPS is and why it is needed.

2. IP blocking identified as Botnet & C&C must be activated

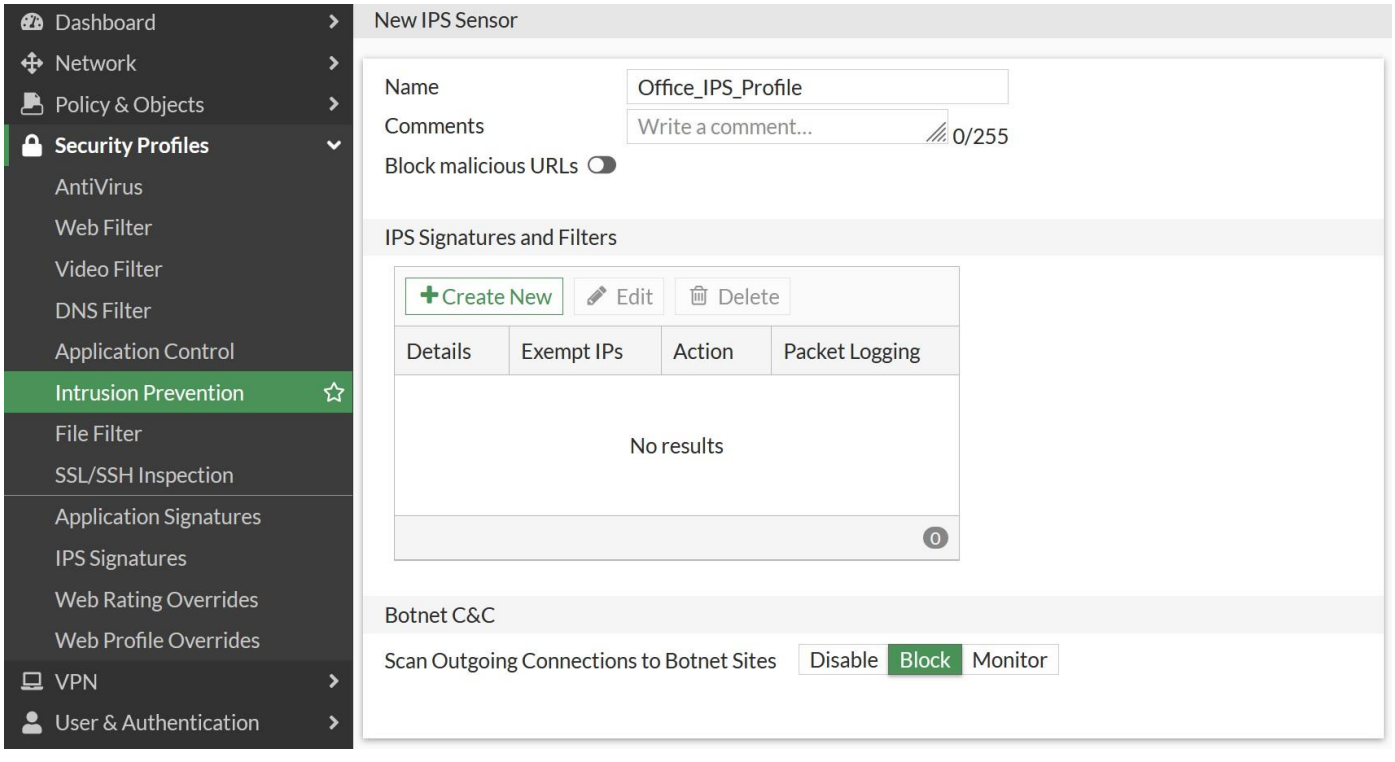
IPS - Intrusion Prevention System

IPS is a network security technology that monitors network traffic for suspicious activities or known attack patterns and takes action to block or prevent them. In FortiGate, IPS is essential for proactively identifying and blocking malicious activities, such as unauthorized access attempts, malware infections, and network-based attacks.

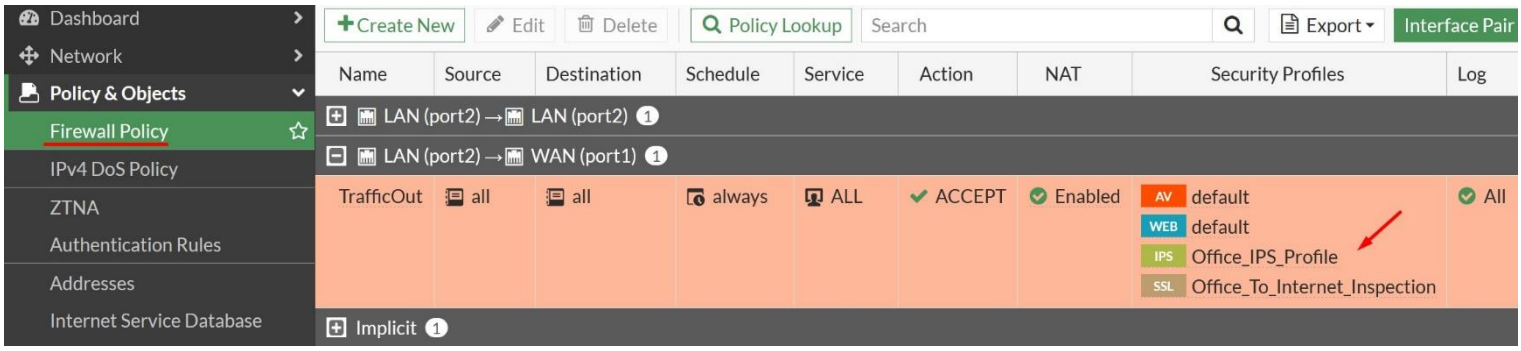
It helps fortify network defenses by detecting and mitigating threats in real-time, enhancing overall security posture and protecting against potential data breaches or system compromises.

Let’s start.

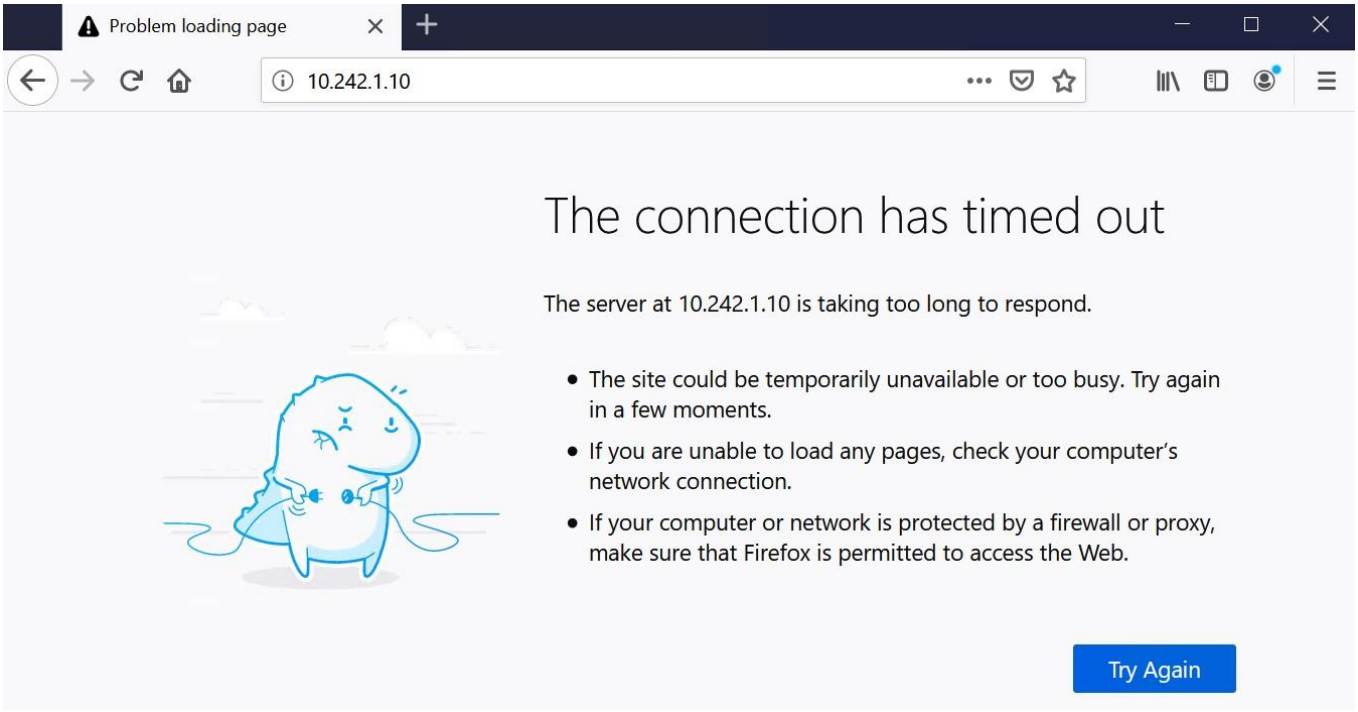
we will Create a new profile and enable botnet blocking.



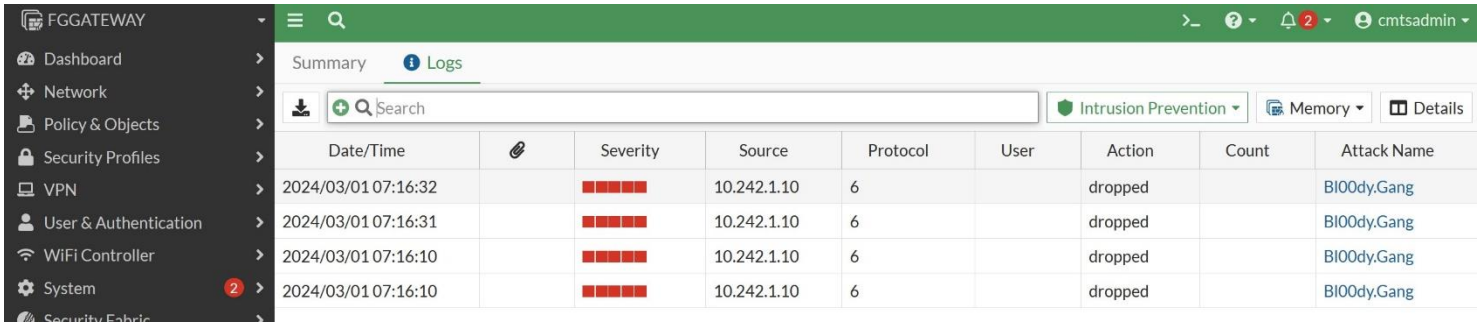
Adding a new IPS profile to the policy



We take a malicious site and test a new inspection via PC.



We also check the LOGS



Application – Control

- An Office_Application_Control profile must be created

1. Block TeamViewer

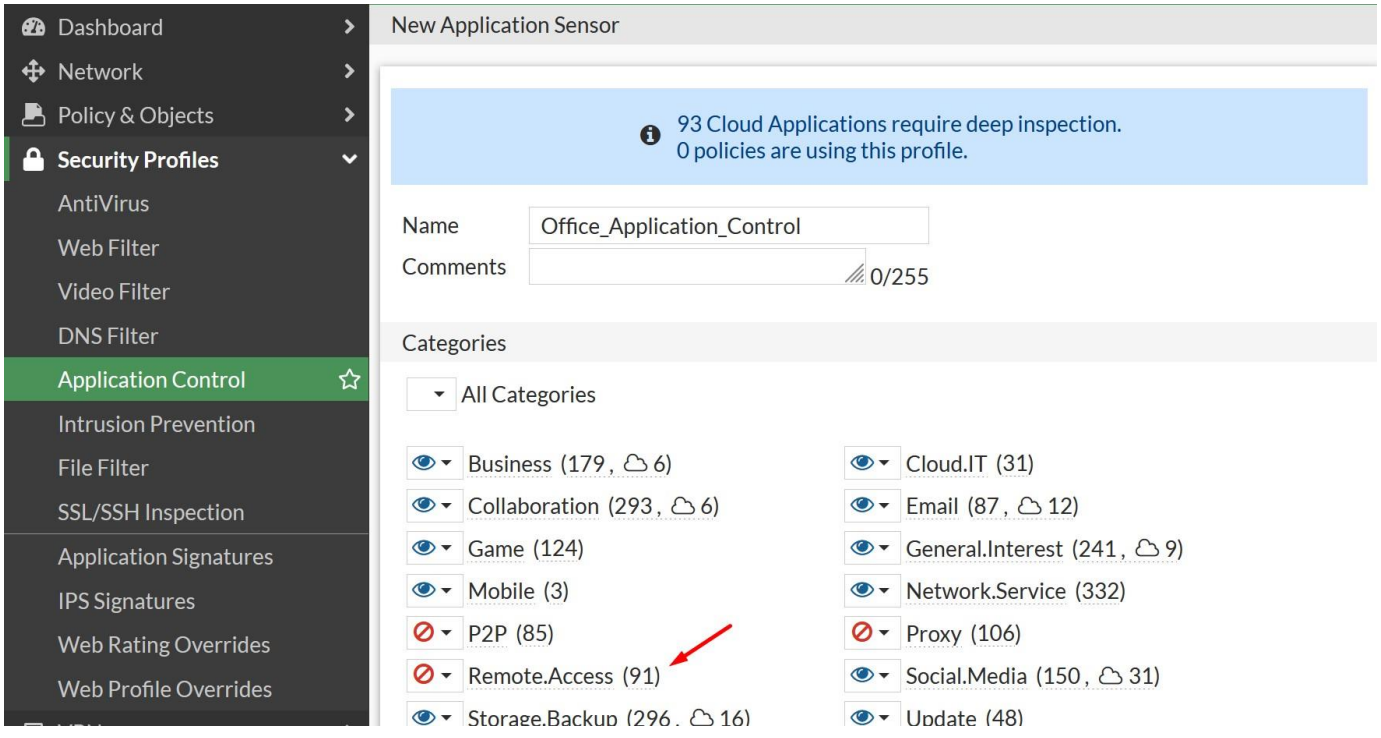
2. Create a situation where a user who accesses a site that we defined as forbidden will be blocked for two days.

Application control in FortiGate allows administrators to monitor, control, and manage the applications running on their networks. It identifies applications using deep packet inspection and signature-based detection, enabling granular control over their usage.

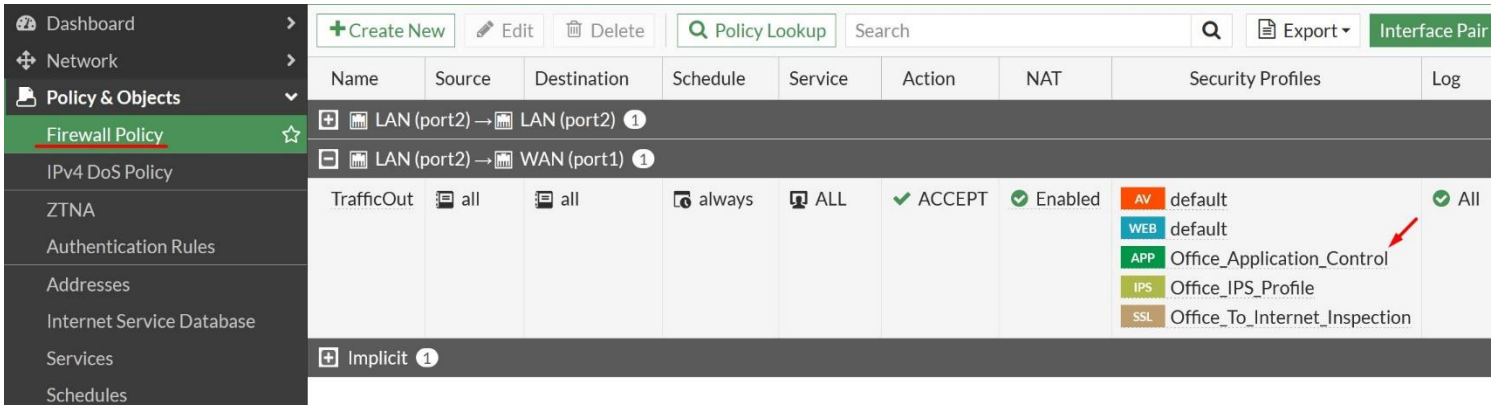
This control is crucial for security, threat prevention, bandwidth management, and enforcing network usage policies.

System administrators can enforce policies on the application and block certain services in the application and enable.

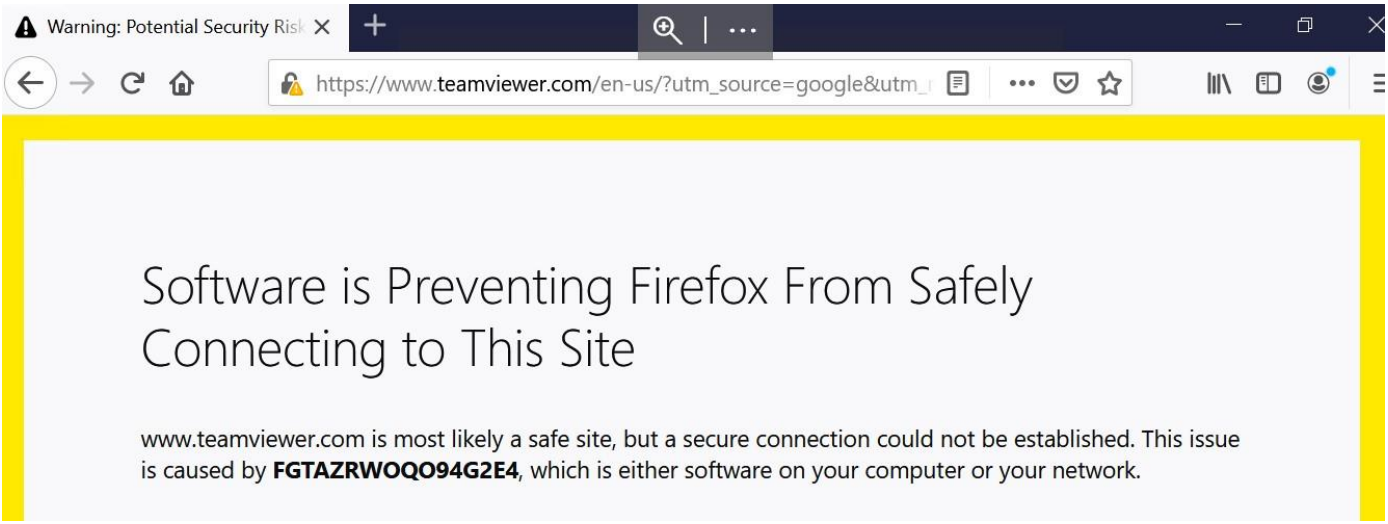
We will create a new profile in Application Control tab, We give a name and prohibit the remote access category that includes the Team Viewer application



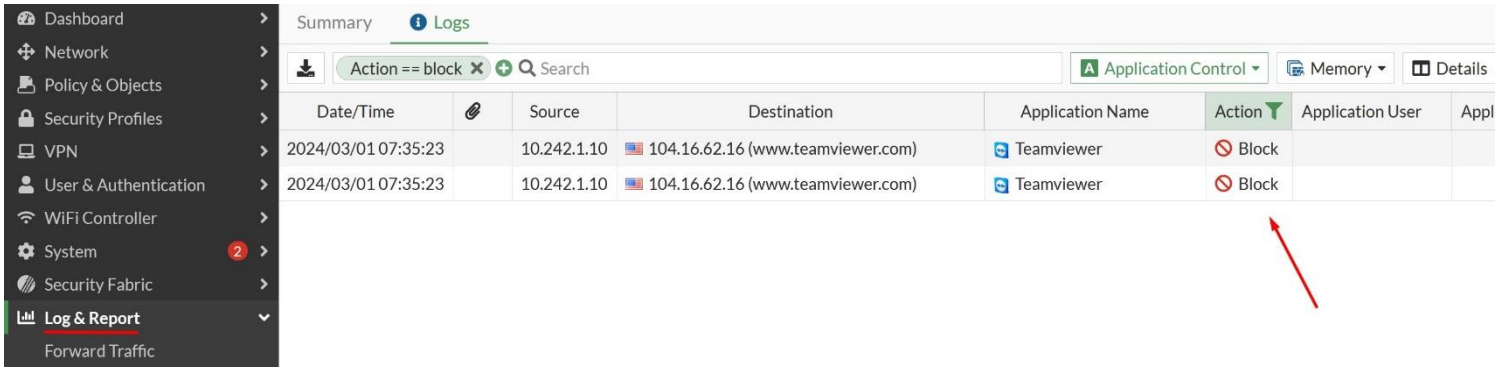
We also send this profile to our policy.



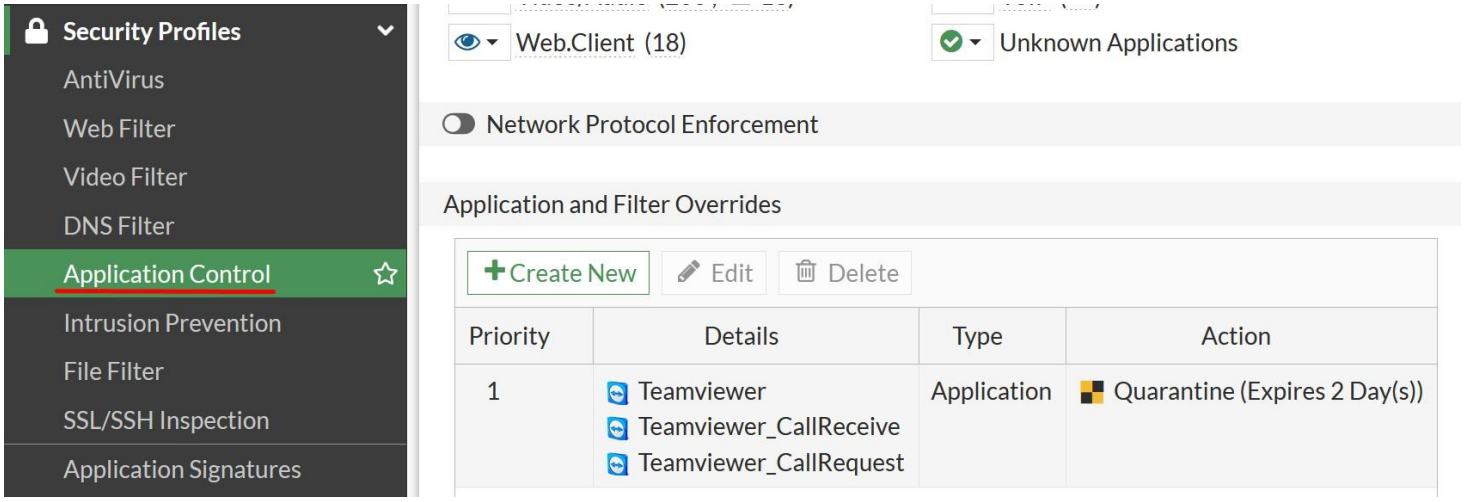
We are going to the workstation and go to the application website, we see that the profile is working



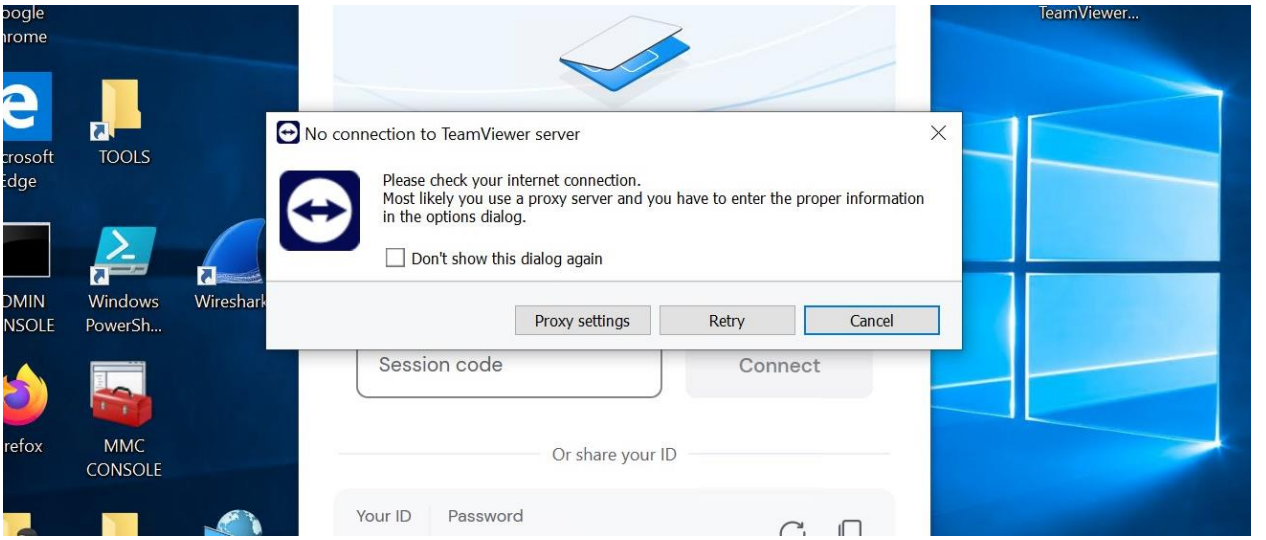
Also check the logs



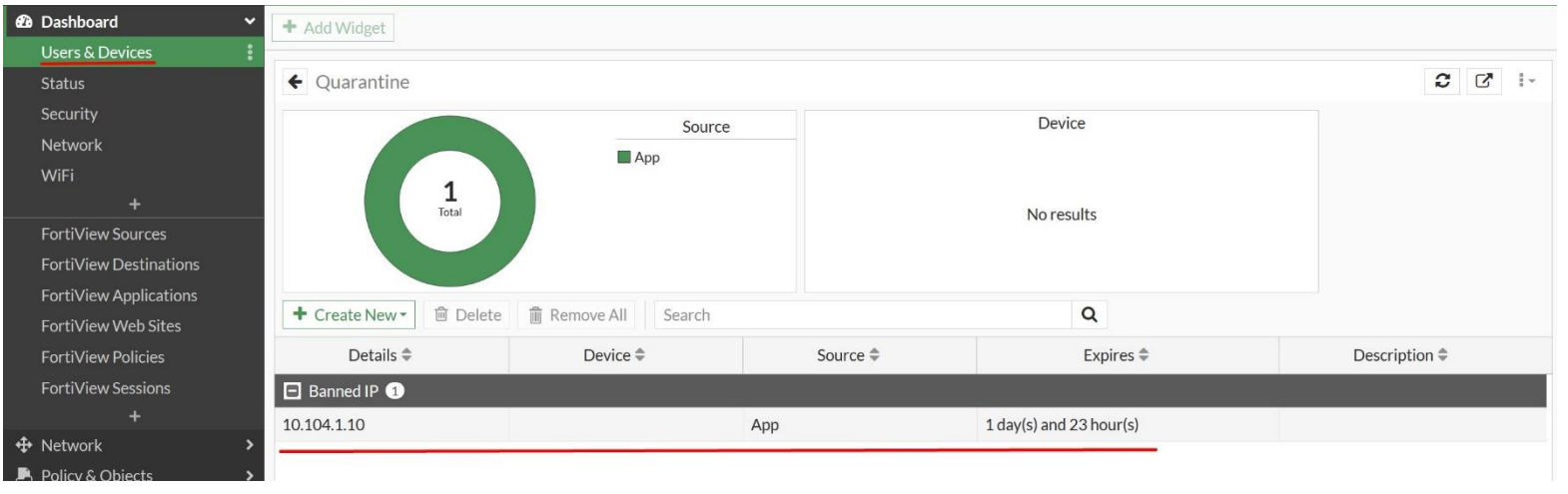
Now the task is to quarantine the user for two days who uses this application, we move to our profile again and choosing Quarantine for 2 days



Let's check this:



We go to the dashboard and see that the user has been quarantined



In FortiGate’s

Application control profile - quarantine mode automatically isolates network traffic that matches defined criteria, redirecting it to a designated quarantine area for further inspection and action by administrators.

You can also cancel this quarantine at Dashboard>User & Devices