

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

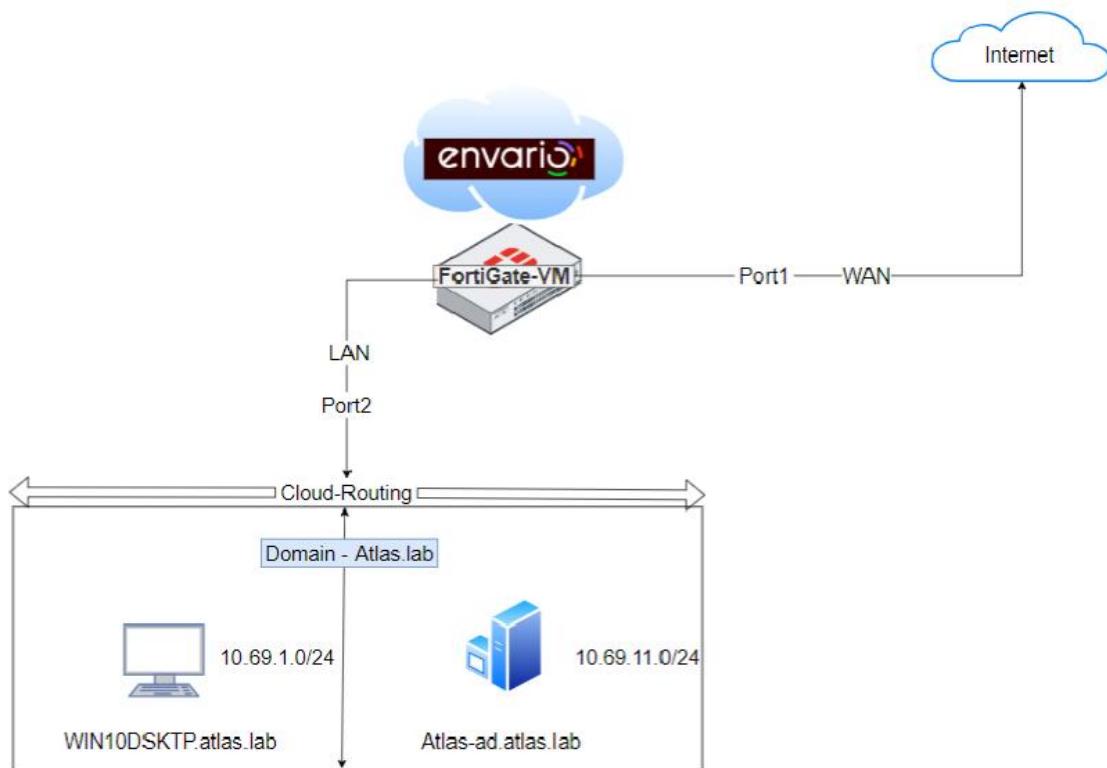
Topology	3
What is FortiGate?	4
Where is it used?	4
User Management.....	5
Password Policy	9
VPN: SSLVPN Tunnel Mode	10
How RDP and VPN works?	21
VPN: SSLVPN Web Mode	22
Virtual IP	27
What is Loopback address?.....	29
IPsec	31
SSL/TLS Inspection	37
Web-Filter	39
DNS-Filter.....	43
Antivirus – Profile	46
IPS – Profile	48
Application – Control	50

Topology

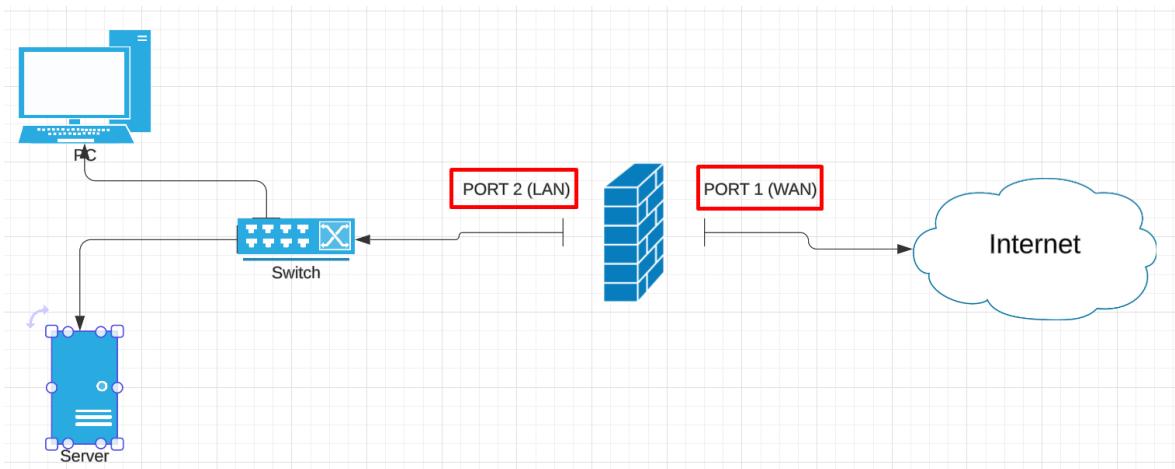
In this work we will use virtual machines on the ENVARIO website.
Now let's talk about topologies.

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?

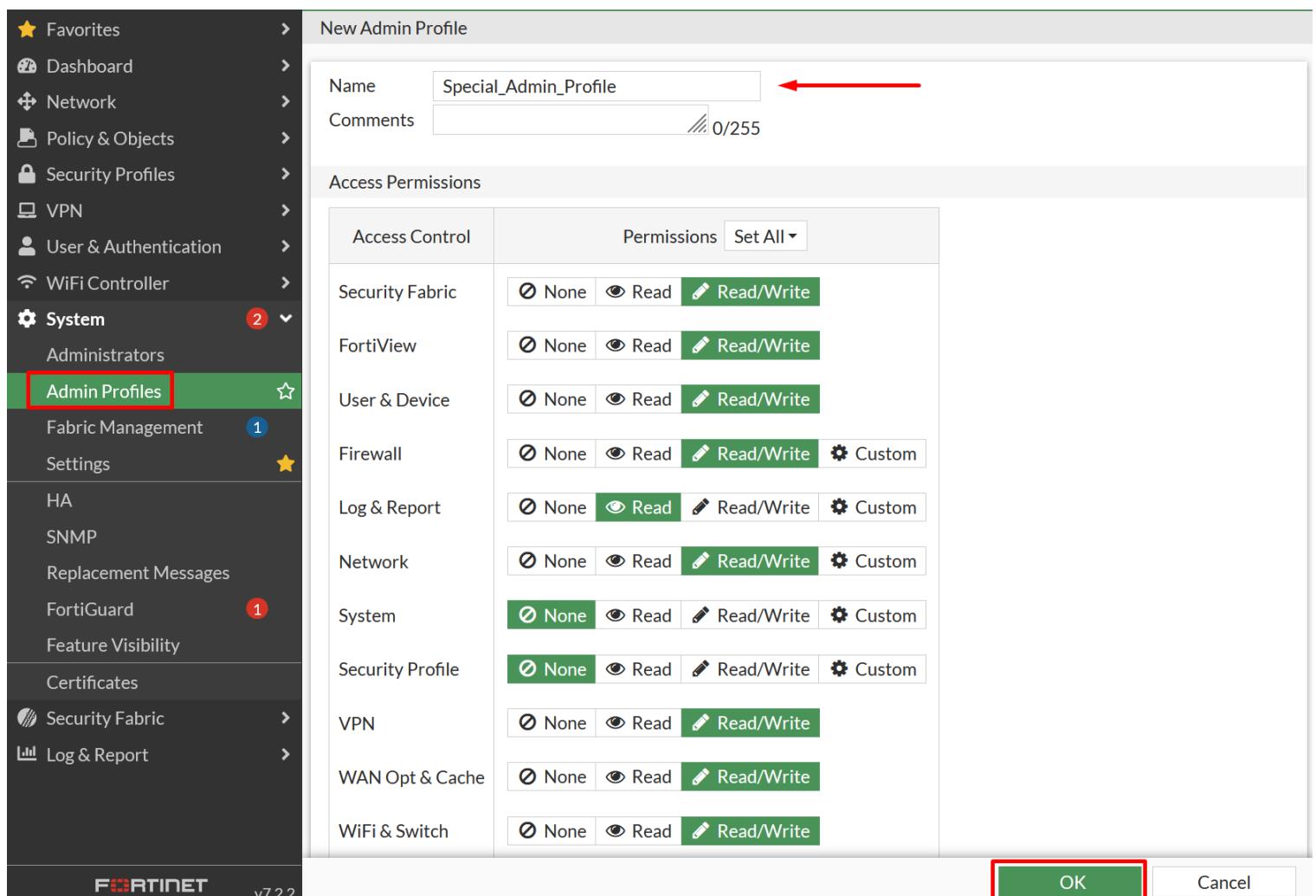
FortiGate appliances are widely used in enterprise networks, data centers, and service provider environments to secure network traffic and ensure the confidentiality, integrity, and availability of data and resources. They are available in various models and configurations to meet the specific security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



The screenshot shows the FortiManager interface for creating a new admin profile. The left sidebar is dark grey with white icons and text, showing various system and network management options. A red box highlights the 'Admin Profiles' option under the 'System' section. To its right, a green box highlights the 'Fabric Management' option. A blue circle with the number '1' is next to 'Fabric Management'. Another blue circle with the number '2' is next to the 'System' icon. The main window has a light grey header 'New Admin Profile'. The 'Name' field contains 'Special_Admin_Profile' with a red arrow pointing to it. The 'Comments' field is empty with '0/255' characters available. Below this is a table titled 'Access Permissions' with a 'Permissions' dropdown set to 'Set All'. The table lists ten categories: Security Fabric, FortiView, User & Device, Firewall, Log & Report, Network, System, Security Profile, VPN, WAN Opt & Cache, and WiFi & Switch. Each category has four permission levels: None (disabled), Read (green), Read/Write (green), and Custom (disabled). The 'Log & Report' row shows 'Read' and 'Read/Write' are enabled. The bottom right of the dialog has an 'OK' button with a red border and a 'Cancel' button.

- 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

New Administrator

Username: Special_Admin

Type: Local User

Password: [REDACTED]

Confirm Password: [REDACTED]

Comments: Administrator profile: Special_Admin_Profile

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

This FortiGate is subject to a critical severity vulnerability. Immediate upgrade is recommended.

Date/Time

Result Policy ID

Memory Details

Special_Admin

Certificates

SSL/SSH Inspection

Memory Details

Result Policy ID

- 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.

New Admin Profile

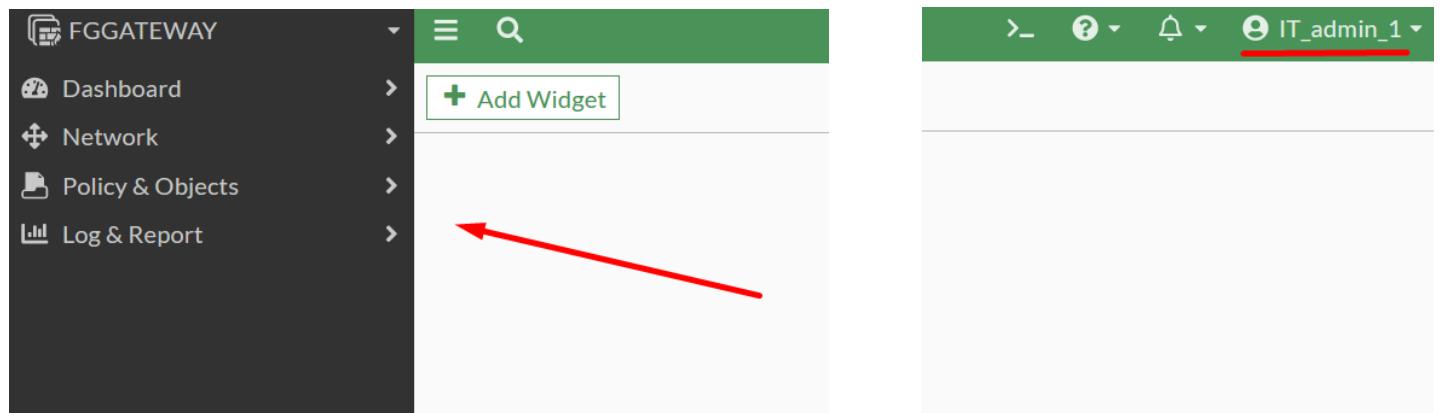
Name	IT_Group
Comments	0/255
Access Permissions	
Access Control	Permissions Set All ▾
Security Fabric	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
FortiView	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
User & Device	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Firewall	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>
Policy	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Address	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Service	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Schedule	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Others	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Log & Report	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>
Network	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>
Configuration	<input type="button" value="None"/> <input type="button" value="Read"/> <input type="button" value="Read/Write"/>

- 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.

The screenshot shows the FortiGate UI interface. On the left, there is a navigation sidebar with various settings like WiFi Controller, System, Administrators, Admin Profiles, Fabric Management, Settings (selected), HA, SNMP, Replacement Messages, and FortiGuard. A red arrow points to the 'Settings' tab. On the right, a detailed configuration page for 'Password Policy' is displayed. The 'Character requirements' section is enabled (green switch). It specifies the following requirements:

Requirement	Value
Upper case	2
Lower case	1
Numbers (0-9)	1
Special	2

The 'Password scope' dropdown is set to 'Both' (highlighted with a green box and a red arrow). Other options in the dropdown are 'Off', 'Admin', and 'IPsec'. The 'Minimum length' is set to 8, and the 'Minimum number of new characters' is set to 0.

VPN: SSLVPN Tunnel Mode

- A tunnel connection must be created with LDAP - 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.

The screenshot shows the Windows Active Directory Users and Computers interface. On the left, the navigation pane shows the domain structure under 'atlas.lab'. A red arrow points to the 'LDAP_users' folder. In the center, the 'LDAP_Sales Properties' window is open. It displays the 'Members' tab, which lists three users: User 1, User 2, and User 3, all belonging to the 'atlas.lab/LDAP_users' group.

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

The screenshot shows the FortiGate configuration interface under 'User & Authentication'. The 'LDAP Servers' option is selected. On the right, the 'Edit LDAP Server' dialog is open, showing the following configuration:

- Name: AtlasAD_LDAP
- Server IP/Name: 10.241.11.200
- Server Port: 389
- Common Name Identifier: sAMAccountName
- Distinguished Name: dc=atlas,dc=lab
- Bind Type: Regular (selected)
- Username: atlasadmin@atlas.lab
- Password: (redacted)
- Secure Connection: Off
- Connection status: Successful

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

The screenshot shows the 'User & Authentication' section of the Fortigate interface. Under 'User Definition', 'User Groups' and 'Guest Management' are listed. On the right, the 'Users/Groups Creation Wizard' is open at step 1: 'User Type'. The 'Remote LDAP User' option is selected and highlighted in green. A red arrow points to this selection. Other options include Local User, Remote RADIUS User, Remote TACACS+ User, FSSO, and FortiNAC User.

Choose our server.

The screenshot shows the 'User & Authentication' section of the Fortigate interface. Under 'User Definition', 'User Groups' and 'Guest Management' are listed. On the right, the 'Users/Groups Creation Wizard' is open at step 2: 'LDAP Server'. The 'AtlasAD_LDAP' server is selected and highlighted in green. A red arrow points to this selection. The interface includes a search bar and a 'Create' button.

Next we need to select new users from the Active Directory

The screenshot shows the 'Users/Groups Creation Wizard' interface. On the left, a sidebar menu includes 'User & Authentication' under 'User Definition'. The main window displays a tree view of an LDAP directory structure under 'dc=atlas,dc=lab'. A red arrow points from the tree view to the right panel, which lists selected users: 'user1', 'user2', and 'user3', all highlighted in yellow.

ID	Name
atlasadmin	atlasadmin
DefaultAccount	DefaultAccount
Guest	Guest
krbtgt	krbtgt
user1	User 1
user2	User 2
user3	User 3

And check that they have been added to the user category

The screenshot shows the 'User Definition' page. The 'User & Authentication' section is selected in the sidebar. The main table lists users with their names, types (LOCAL or LDAP), and two-factor authentication status. The rows for 'user1', 'user2', and 'user3' are highlighted in yellow and enclosed in a red box, indicating they have been successfully added.

Name	Type	Two-factor Authentication
guest	LOCAL	✗
user1	LDAP	✗
user2	LDAP	✗
user3	LDAP	✗

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.

Name: tunnel-access

Tunnel Mode:

- 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.

Source IP Pools:

- AtlasAD
- SSLVPN_TUNNEL_ADDR1

● 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.

- AtlasAD
- SSLVPN_TUNNEL_ADDR1

Address	SSLVPN_TUNNEL_ADDR1
Type	IP Range
IP Range	10.212.134.200 - 10.212.134.210
Interface	any
References	2

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

The screenshot shows a network configuration interface with a sidebar on the left containing icons for Favorites, Dashboard, Network, Policy & Objects, Security Profiles, VPN, Overlay Controller VPN, IPsec Tunnels, IPsec Wizard, IPsec Tunnel Template, and SSL-VPN Portals. The 'SSL-VPN Portals' item is highlighted with a green bar at the bottom of the sidebar.

The main area displays a table with three columns: Name, Tunnel Mode, and Web Mode. The table has three rows:

Name	Tunnel Mode	Web Mode
full-access	Enabled	Enabled
tunnel-access	Enabled	Disabled
web-access	Disabled	Enabled

The 'tunnel-access' row is highlighted with a red box around its entire row. The 'Enabled' checkbox in the 'Tunnel Mode' column for 'tunnel-access' is also highlighted with a red box.

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

The screenshot shows the FortiGate User & Authentication interface. On the left sidebar, under 'User Groups', 'User Groups' is selected. In the main panel, a 'New User Group' dialog is open. The 'Name' field contains 'LDAP_Users' with a red arrow pointing to it. The 'Type' dropdown menu is open, showing 'Firewall' (selected), 'Fortinet Single Sign-On (FSSO)', 'RADIUS Single Sign-On (RSSO)', and 'Guest'. Below the type selection is a 'Members' input field with a '+' button. At the bottom of the dialog is a 'Remote Groups' section with 'Add', 'Edit', and 'Delete' buttons, and a table listing a single entry: 'AtlasAD_LDAP'.

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

The screenshot shows the FortiGate SSL-VPN Settings interface. On the left sidebar, 'SSL-VPN Settings' is selected. In the main panel, the 'Connection Settings' section is visible. Under 'Listen on Interface(s)', 'WAN (port1)' is selected with a red arrow pointing to it. Under 'Listen on Port', '443' is listed. A tooltip indicates 'Web mode access will be listening at https://10.241.254.254:443'. In the 'Server Certificate' dropdown, 'Fortinet_Factory' is selected with a red arrow pointing to it. A warning message states: 'You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one.' A 'Create Certificate' button is present. At the bottom, there are tabs for 'Allow access from any host' and 'Limit access to specific hosts'.

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

Tunnel Mode Client Settings

Address Range: Automatically assign addresses

DNS Server: Same as client system DNS

Web Mode Settings

Language: Browser preference

Authentication/Portal Mapping

Users/Groups	Portal
LDAP_Users	tunnel-access
All Other Users/Groups	Not Set

SSL-VPN Settings

Restrict Access: Allow access from any host

Tunnel Mode Client Settings

Address Range: Automatically assign addresses

DNS Server: Same as client system DNS

New Authentication/Portal Mapping

Users/Groups	Portal
LDAP_Users	tunnel-access

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)

The screenshot shows a navigation menu on the left with the following items:

- Favorites
- Dashboard
- Network
- Policy & Objects
- Firewall Policy (highlighted in green)
- IPv4 DoS Policy
- ZTNA
- Authentication Rules
- Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs
- IP Pools
- Protocol Options

The main panel is titled "New Policy" and contains the following configuration fields:

- Name: SSLVPN_Tunnel_Access
- Incoming Interface: SSL-VPN tunnel interface (ssl.root)
- Outgoing Interface: LAN (port2)
- Source:
 - SSLVPN_TUNNEL_ADDR1
 - LDAP_Users
- Destination:
 - win10wrk1
- Schedule: always
- Service: RDP
- Action:
 - ACCEPT (selected)
 - DENY

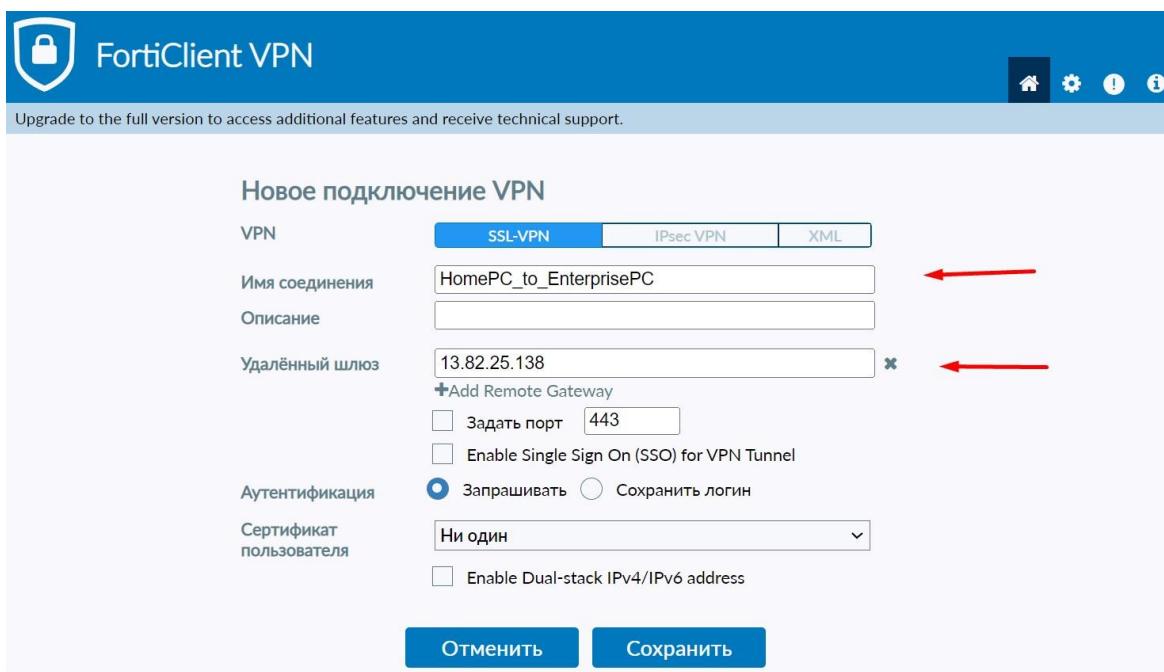
At the bottom, there is an "Inspection Mode" section with "Flow-based" selected over "Proxy-based".

Let's check if its works.

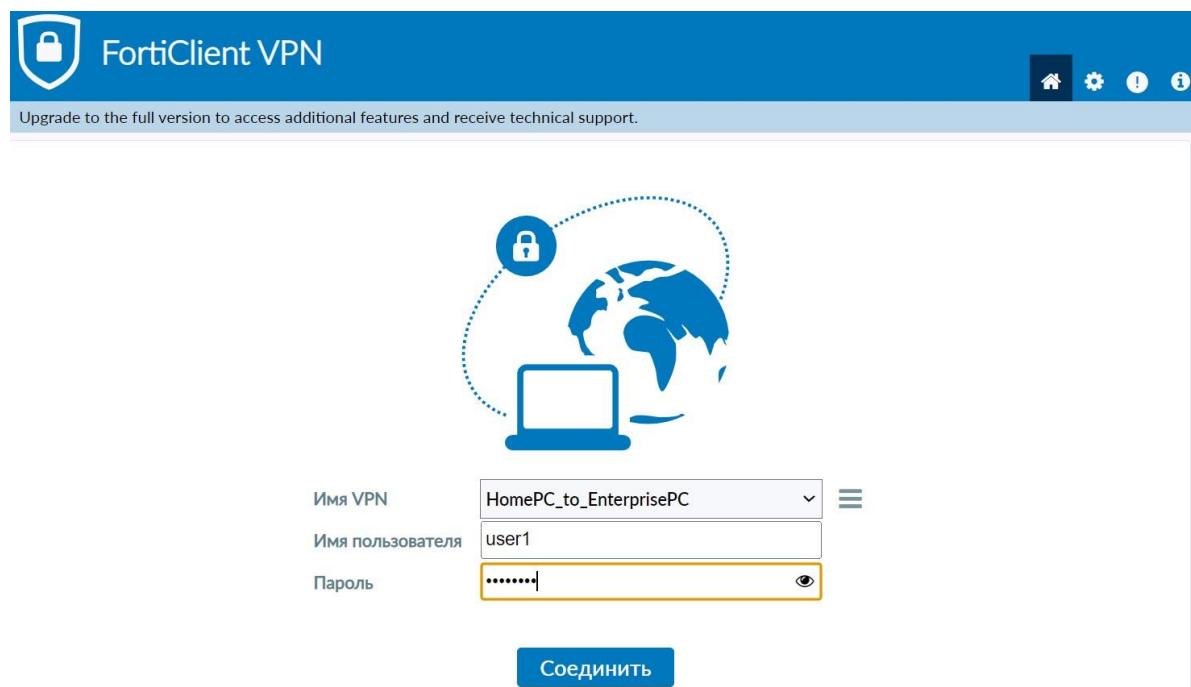
First, we need to install the FortiClient VPN on the computer to connect remotely and safely to the workstation.

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

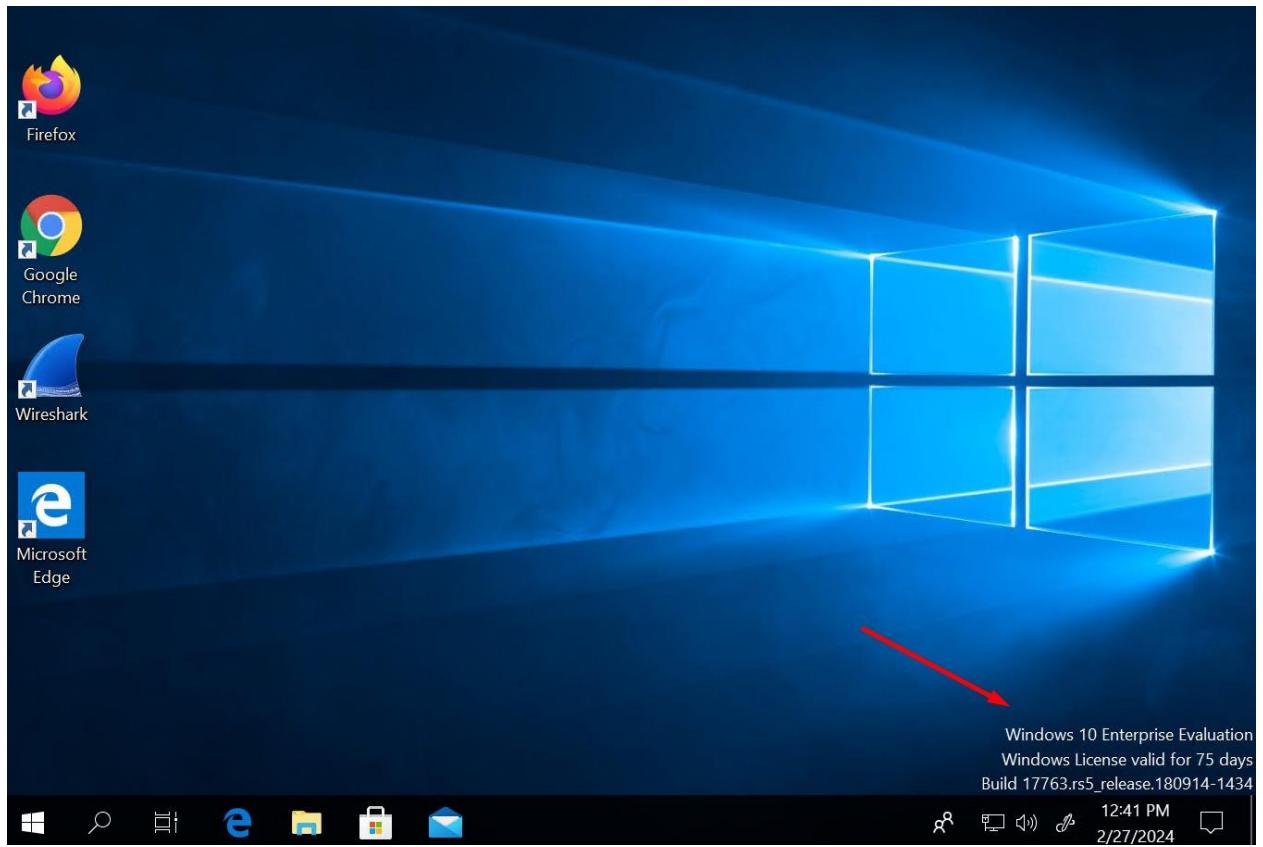
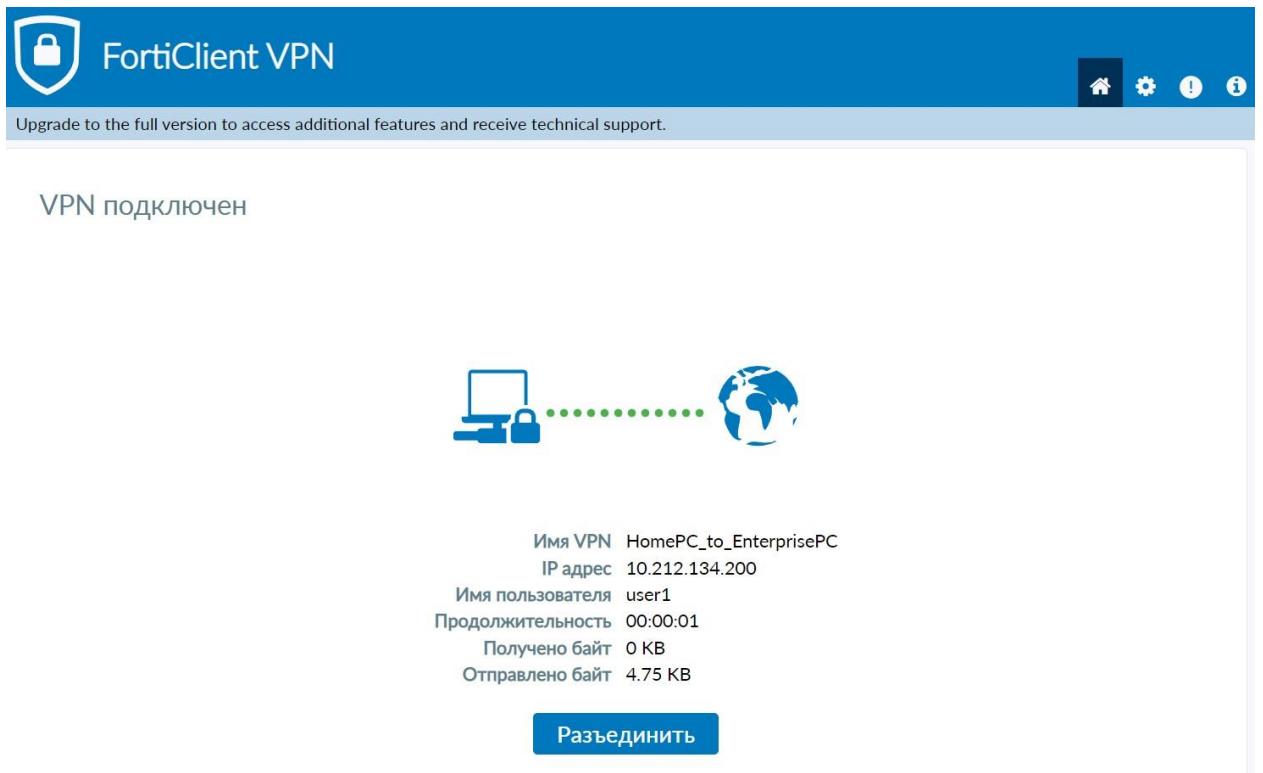
We give the name of our session, in our case it is from a home PC to the company's workstation, we register the remote Default Gateway of FortiGate, where the traffic will flow. After this, we leave the default port 443/HTTPS since we did not change it in the SSLVPN settings.



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 rule 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)

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane shows the tree structure of the domain 'atlas.lab'. In the center, a list of objects is displayed, including a security group named 'LDAP_HR' and several user accounts ('User 1', 'User 2', 'User 3'). On the right, a detailed view of the 'LDAP_HR' group properties is shown in a modal window titled 'LDAP_HR Properties'. The 'Members' tab is selected, displaying a table of members. Three user accounts ('User HR 1', 'User HR 2', 'User HR 3') are listed, each associated with the path 'atlas.lab/LDAP_users'. The entry for 'User HR 1' is highlighted with a red box.

Name	Type
LDAP_HR	Security Group...
LDAP_Sales	Security Group...
User 1	User
User 2	User
User 3	User
User HR 1	User
User HR 2	User
User HR 3	User

Name	Active Directory Domain Services Folder
User HR 1	atlas.lab/LDAP_users
User HR 2	atlas.lab/LDAP_users
User HR 3	atlas.lab/LDAP_users

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

The screenshot shows the 'Edit SSL-VPN Portal' configuration page. The left sidebar has a 'SSL-VPN Portals' section selected. The main area shows the 'Edit SSL-VPN Portal' configuration. The 'Name' field is set to 'web-access'. The 'Web Mode' option is selected. In the 'Predefined Bookmarks' section, there is a 'Create New' button highlighted with a red box. A red arrow points to the 'Name' field in the 'Create New' dialog.

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.

The screenshot shows the 'New Bookmark' dialog box. It contains fields for Name (WebAccess_PC), Type (RDP), Host (10.241.1.10), Port (3389), Description (Single Sign-On), Username, Password, Color depth (16 Bit selected), Screen width, Screen height, Keyboard layout, Security (Allow the server to choose the type), and Restricted admin mode. The 'OK' button at the bottom right is highlighted with a red box.

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

The screenshot shows the Fortigate management interface. On the left, the navigation menu is visible with 'User & Authentication' expanded, and 'User Groups' selected. A red arrow points to the 'User Groups' link. The main panel displays the 'New User Group' configuration page. The 'Name' field contains 'LDAP_HR'. The 'Type' dropdown is set to 'Firewall', which is highlighted in green. Below the type dropdown is a list of other options: 'Fortinet Single Sign-On (FSSO)', 'RADIUS Single Sign-On (RSSO)', and 'Guest'. The 'Members' field is empty, indicated by a plus sign. Below this is the 'Remote Groups' section, which lists a single entry: 'AtlasAD_LDAP'. A red arrow points to this entry. At the bottom right of the 'Remote Groups' table, there is a small circled number '1'.

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.

The screenshot shows the Fortigate management interface with the 'SSL-VPN Settings' section selected in the navigation menu. The main panel displays the 'SSL-VPN Settings' configuration page. In the bottom right corner, a modal window titled 'New Authentication/Portal Mapping' is open. The 'Users/Groups' dropdown contains 'LDAP_HR', and the 'Portal' dropdown contains 'web-access'. At the bottom right of the modal are 'OK' and 'Cancel' buttons. The background shows various SSL-VPN settings like 'SSL-VPN Portals', 'Tunnel Mode Client Settings', and 'Web Mode Settings'.

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

The screenshot shows a left-hand navigation menu with various system and security-related options. The 'Firewall Policy' option is selected and highlighted in green. On the right, a 'New Policy' dialog box is open, prompting for configuration details. The 'Name' field is set to 'SSLVPN_Web_Access'. The 'Incoming Interface' is specified as 'SSL-VPN tunnel interface (ssl.root)'. The 'Outgoing Interface' is set to 'LAN (port2)'. Under 'Source', two entries are listed: 'SSLVPN_TUNNEL_ADDR1' and 'LDAP_HR', each with a '+' button to add more. Under 'Destination', there is one entry: 'win10wrk1', also with a '+' button. The 'Schedule' is set to 'always', and the 'Service' is set to 'ALL'. At the bottom of the dialog, there are 'ACCEPT' and 'DENY' buttons, with 'ACCEPT' being checked. Below the dialog, the 'Inspection Mode' is set to 'Flow-based', and 'Proxy-based' is also an option. Further down, under 'Firewall/Network Options', the 'NAT' toggle switch is turned off. The 'Protocol Options' dropdown is set to 'PROT default', with a pencil icon for editing.

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

Please Login

userhr1
••••••••••
Login
Launch FortiClient

00:06:35 0 B+ 6.41 kB+

SSL-VPN Portal

👤 Launch FortiClient 📲 Download FortiClient

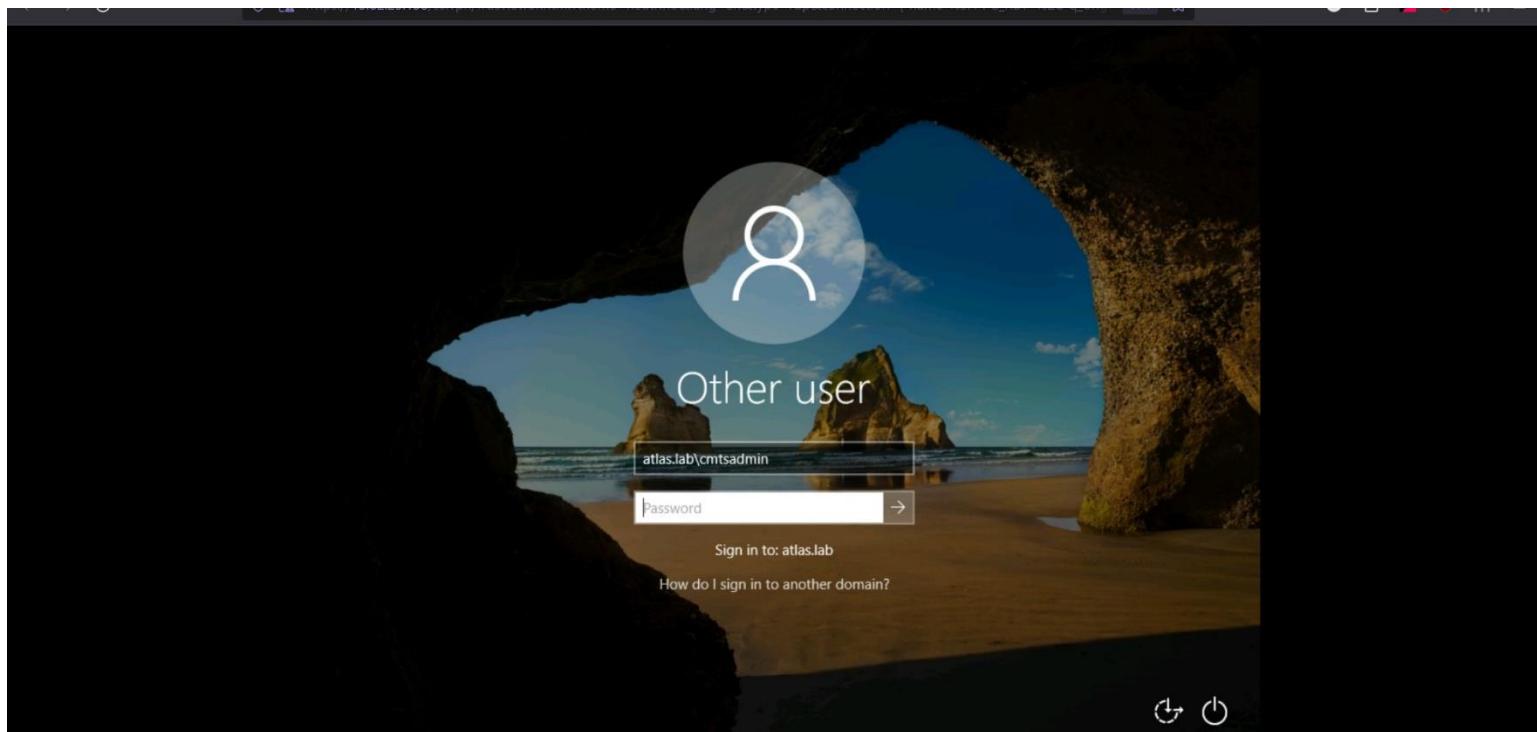
Your Bookmarks

💻 PC_RDP

🔗 Quick Connection + New Bookmark

History

Date	IP Address	Duration	Bandwidth
2024/02/27 16:09:04	87.71.172.218	6 second(s)	0 B in / 0 B out
2024/02/27 16:05:22	87.71.172.218	3 minute(s) and 32 second(s)	0 B in / 0 B out



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?

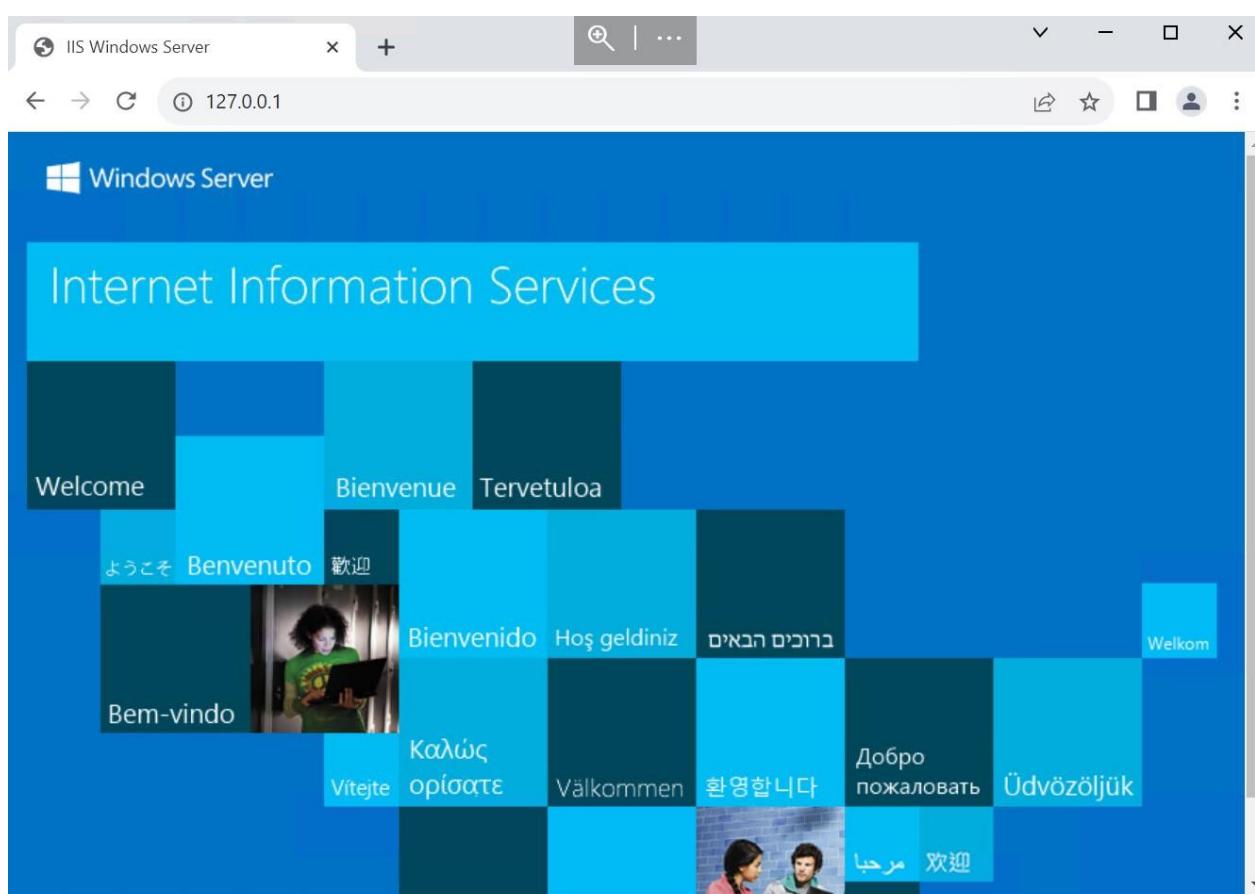
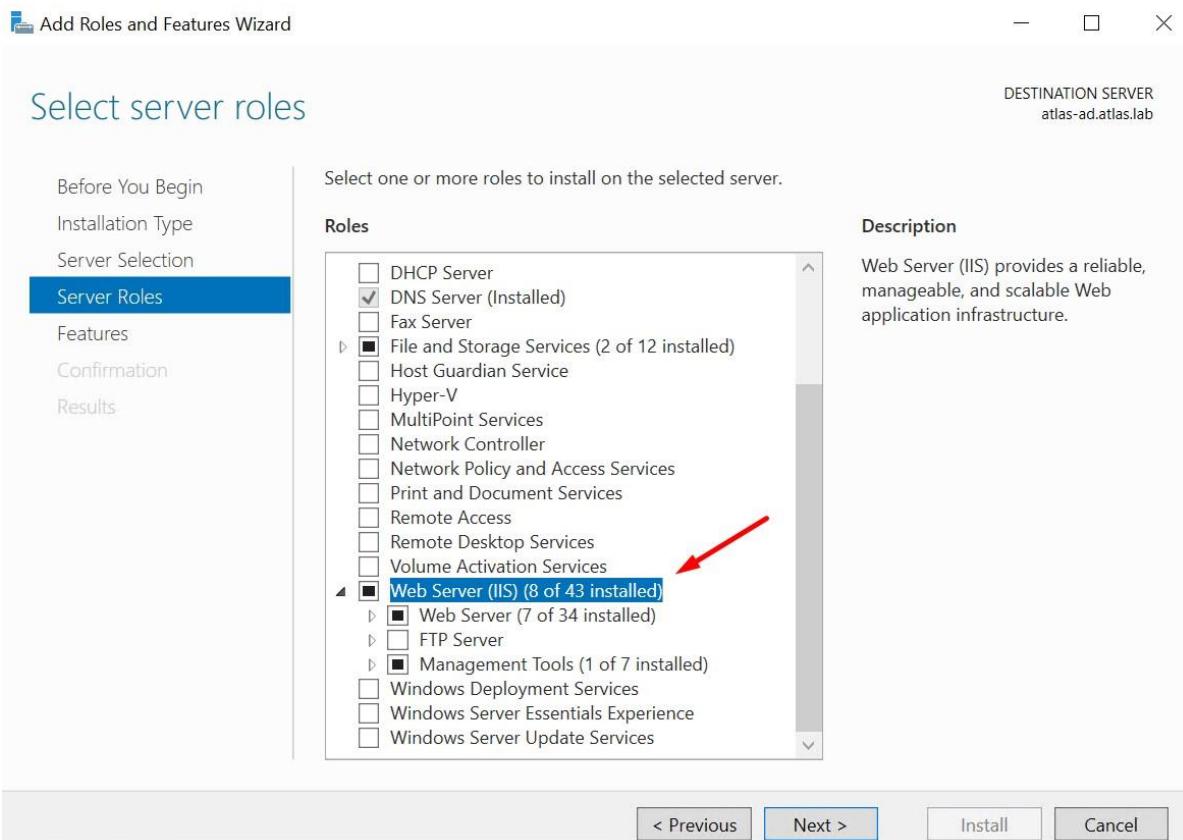
VIP stands for Virtual IP. It's a feature that allows mapping multiple public IP addresses to private IP addresses on your network. This enables services running on internal servers, such as **web servers** or email servers, to be accessible from the internet using different public IP addresses.

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.

The screenshot shows the FortiGate management interface at the URL <https://13.82.25.138:8443/ng/firewall/virtual-ip/vip/edit/Website>. The left sidebar is a navigation menu with the following items:

- Favorites
- Interfaces
- Firewall Policy
- Virtual IPs** (selected)
- IPsec Tunnels
- System Settings
- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- WiFi Controller

The main content area is titled "Edit Virtual IP". It contains the following fields:

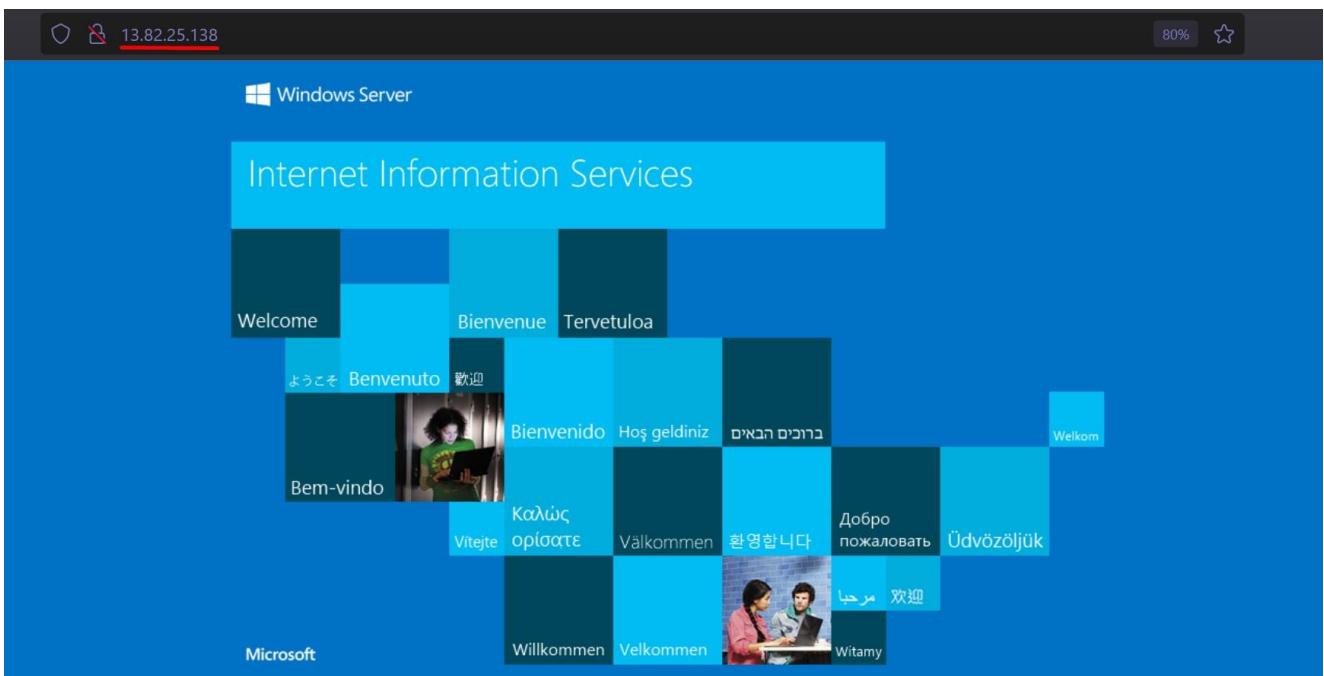
VIP type	IPv4
Name	Website
Comments	Write a comment... 0/255
Color	Change
Network	
Interface	WAN (port1)
Type	Static NAT
External IP address/range	10.241.254.254 FortiGate
Map to	IPv4 address/range 10.241.11.200 AtlasAD

A red banner at the top right of the content area states: "This FortiGate is subject to a critical severity vulnerability. Immediate upgrade is recommended." with a link icon.

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)

The screenshot shows a left sidebar with navigation options like Favorites, Dashboard, Network, Policy & Objects (selected), Firewall Policy (selected), IPv4 DoS Policy, ZTNA, Authentication Rules, Addresses, Internet Service Database, Services, Schedules, and Virtual IPs. The main area is titled 'New Policy' and contains fields for Name (Access_to_WEB), Incoming Interface (WAN (port1)), Outgoing Interface (LAN (port2)), Source (all), IP/MAC Based Access Control (Website), Destination (always), Service (Web Access), and Action (ACCEPT selected). At the bottom are 'ACCEPT' and 'DENY' buttons.

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

NYC_to_TLV

Site to Site Hub-and-Spoke Remote Access Custom

No NAT between sites

This site is behind NAT
The remote site is behind NAT

FortiGate Cisco

Site to Site - FortiGate

This FortiGate

Internet

Remote FortiGate

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.

13.82.92.101

WAN (port1)

Pre-shared Key Signature

Abcd1234IPSEC!@

Site to Site - FortiGate

This FortiGate

Internet

Remote FortiGate

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

The screenshot shows the 'VPN Creation Wizard' interface for a 'Site to Site - FortiGate' connection. The left sidebar lists various VPN-related options like Dashboard, Network, Policy & Objects, Security Profiles, VPN, Overlay Controller VPN, IPsec Tunnels, and IPsec Wizard. The IPsec Wizard is currently selected. The main window displays the 'Policy & Routing' step (step 3 of 4). It shows the Local interface as 'LAN (port2)', Local subnets as '10.90.1.0/24' and '10.90.11.0/24', and Remote Subnets as '10.74.1.0/24' and '10.74.11.0/24'. An 'Internet Access' section indicates 'None'. On the right, a diagram shows two FortiGates connected via the Internet, with one labeled 'This FortiGate'.

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.

The screenshot shows the 'IPsec Monitor' section of the FortiView interface. The left sidebar includes options like Dashboard, Status, Security, Network, Users & Devices, WiFi, and IPsec Monitor. The IPsec Monitor is selected. The main area displays an IPsec connection named 'NYC_to_TLV' with a remote gateway of '13.82.92.101'. The connection status is shown as '0 B' for both incoming and outgoing data. A context menu is open over the connection entry, with the 'Phase 2 Selectors' option highlighted. A sub-menu for 'Phase 2 Selector: NYC_to_TLV' is open, showing 'All Phase 2 Selectors'.

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)

Edit Policy

Name: vpn_NYC_to_TLV_local_0

Incoming Interface: LAN (port2)

Outgoing Interface: NYC_to_TLV

Source: NYC_to_TL_local

Destination: NYC_to_TL_remote

Schedule: always

Service: PING

Action: ACCEPT

Select Entries

Q:ping

SERVICE (1)

Network Services (1)

PING

TLV to NYC (Just RDP)

Edit Policy

Name: vpn_NYC_to_TLV_remote_0

Incoming Interface: NYC_to_TLV

Outgoing Interface: LAN (port2)

Source: NYC_to_TL_remote

Destination: NYC_to_TL_local

Schedule: always

Service: ALL

Action: ACCEPT

Select Entries

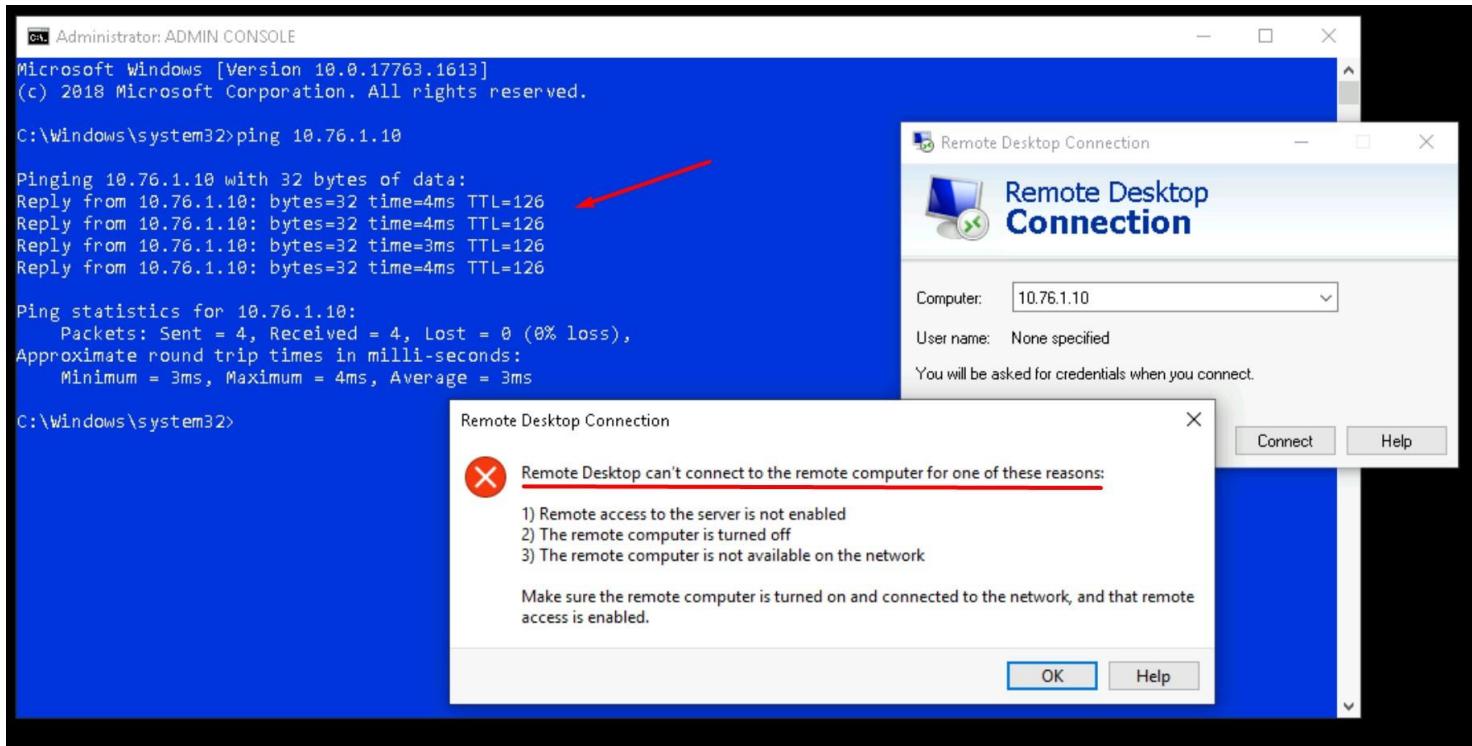
Q:rdp

SERVICE (1)

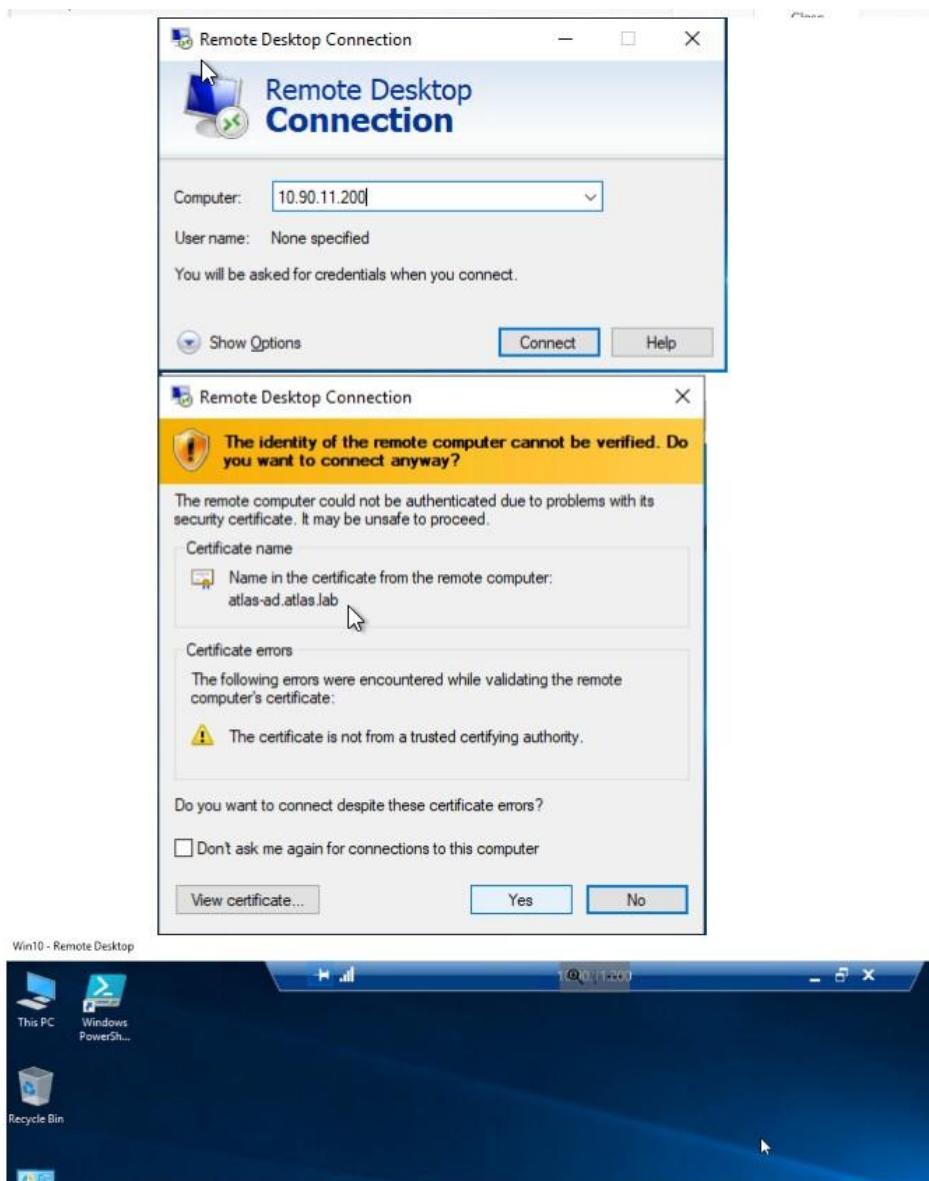
Remote Access (1)

RDP

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



screenshots of my classmate



```
This PC
Administrator: ADMIN CONSOLE
Microsoft Windows [Version 10.0.17763.1613]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.90.11.200

Pinging 10.90.11.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.90.11.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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.

FGGATEWAY

New SSL/SSH Inspection Profile

Name: Office_To_Internet_Inspection

Comments: Write a comment... 0/255

SSL Inspection Options

Enable SSL inspection of: Multiple Clients Connecting to Multiple Servers
Protecting SSL Server

Inspection method: SSL Certificate Inspection (Full SSL Inspection)

CA certificate: Fortinet_CA_SSL (Download)

Blocked certificates: View Blocked Certificates

Untrusted SSL certificates: View Trusted CAs List

Server certificate SNI check: Enable Strict Disable

Enforce SSL cipher compliance: Off

Enforce SSL negotiation compliance: Off

RPC over HTTPS: Off

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

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log
LAN (port2) → LAN (port2)	all	all	always	ACCEPT	Enabled	SSL: Office_To_Internet_Inspection	
LAN (port2) → NYC_to_TLV	all	NYC_to_TLV					
LAN (port2) → WAN (port1)	all	WAN (port1)					
NYC_to_TLV → LAN (port2)	NYC_to_TLV	all					

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.

New Web Filter Profile

Name	Action
custom1	Allow
custom2	Allow

- 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 (*).

Edit Web Filter Profile

Allow users to override blocked categories

Search Engines

Static URL Filter ←

Block invalid URLs

URL Filter

+ Create New	Edit	Delete	Search	Q
URL	Type	Action	Status	0
No results				

New URL Filter

Allow users to override blocked categories

Search Engines

Static URL Filter

Block invalid URLs

URL Filter

+ Create New	Edit
URL <input type="text" value="*.reddit.com"/>	Type <input checked="" type="radio"/> Simple <input type="radio"/> Regular Expression <input checked="" type="radio"/> Wildcard
Action <input type="radio"/> Exempt <input checked="" type="radio"/> Block <input type="radio"/> Allow <input type="radio"/> Monitor	Status <input checked="" type="radio"/> Enable <input type="radio"/> Disable

OK Cancel

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.

Edit Web Filter Profile

Name: Office_Web_Filter
Comments: Write a comment... 0/255
Feature set: Flow-based **Proxy-based**

FortiGuard Category Based Filter

Name	Action
Political Organizations	Allow
Reference	Allow
Global Religion	Allow
Shopping	Authenticate

Edit Filter

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

FortiGuard Category Based Filter

Warning Interval: 0 hour(s) 5 minute(s) 0 second(s)
Selected User Groups: Special_Users

OK **Cancel**

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

Edit Policy

Action: **ACCEPT** DENY

Inspection Mode: **Flow-based** **Proxy-based**

Firewall/Network Options

NAT:

IP Pool Configuration: **Use Outgoing Interface Address** **Use Dynamic IP Pool**

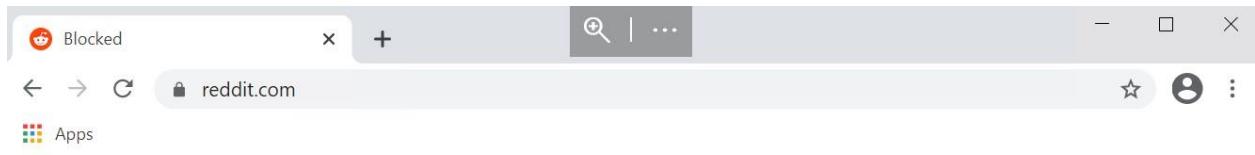
Preserve Source Port:

Protocol Options: PROT default

Security Profiles

AntiVirus: AV default
Web Filter: WEB Office_Web_Filter
Video Filter:

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



whoa there, pardner!

Your request has been blocked due to a network policy.

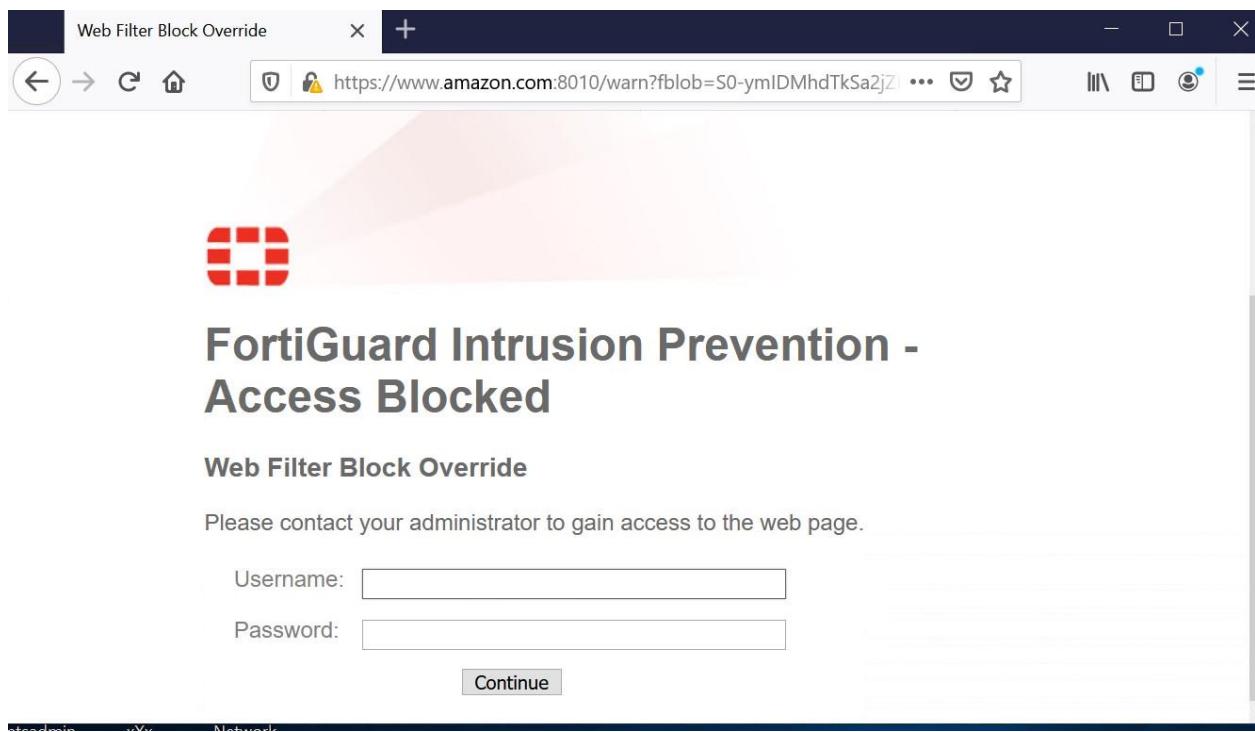
Try logging in or creating an account [here](#) to get back to browsing.

If you're running a script or application, please register or sign in with your developer credentials [here](#). Additionally make sure your User-Agent is not empty and is something unique and descriptive and try again. If you're supplying an alternate User-Agent string, try changing back to default as that can sometimes result in a block.

You can read Reddit's Terms of Service [here](#).

If you think that we've incorrectly blocked you or you would like to discuss easier ways to get the data you want, please file a ticket [here](#).

When contacting us, please include your IP address which is: **40.114.2.138** and reddit account



Logs									
Summary		Logs							
		Date/Time	User	Source	Action	URL	Category	Initiator	Sent / Received
Firewall Policy		2024/03/01 09:17:57		10.104.1.10	Blocked	https://www.reddit.com/favicon.ico			958 B / 0 B
Security Events Log		2024/03/01 09:17:57		10.104.1.10	Blocked	https://www.reddit.com/			1.02 kB / 0 B
Forward Traffic Log		2024/03/01 09:16:42		10.104.1.10	Blocked	https://www.amazon.com/favicon.ico	Shopping		989 B / 0 B
Dashboard		2024/03/01 09:16:41		10.104.1.10	Blocked	https://www.amazon.com/	Shopping		1.02 kB / 0 B

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.

The screenshot shows the FortiGate management interface. On the left, a sidebar lists various security profiles: Dashboard, Network, Policy & Objects, Security Profiles (expanded), AntiVirus, Web Filter, Video Filter, DNS Filter (selected and highlighted in green), Application Control, Intrusion Prevention, File Filter, SSL/SSH Inspection, and Application Signatures. The main panel is titled "New DNS Filter Profile". It contains fields for "Name" (set to "Office_DNS_Filter") and "Comments" (set to "Comments" with a character count of 0/255). A prominent red arrow points to the "Redirect botnet C&C requests to Block Portal" checkbox, which is checked. Below this, a blue callout box displays the message "80000 domains in botnet package". Further down, there are sections for "Enforce 'Safe Search' on Google, Bing, YouTube" and "FortiGuard Category Based Filter". The "FortiGuard Category Based Filter" section includes tabs for "Allow", "Monitor", and "Redirect to Block Portal" (which is selected, indicated by a red circle). A table below shows categories like "Adult/Mature Content" with actions "Allow" and "Block".

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.”

Static Domain Filter

Domain Filter

<input type="button" value="Create New"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	Search	<input type="button" value="Q"/>
Domain	Type	Action	Status	
.facebook.	wildcard	<input type="button" value="X Redirect to Block Portal"/>	<input checked="" type="checkbox"/> Enable	1

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

Dashboard >

Network >

Policy & Objects >

Firewall Policy

IPv4 DoS Policy

ZTNA

Authentication Rules

Addresses

Internet Service Database

Services

Schedule

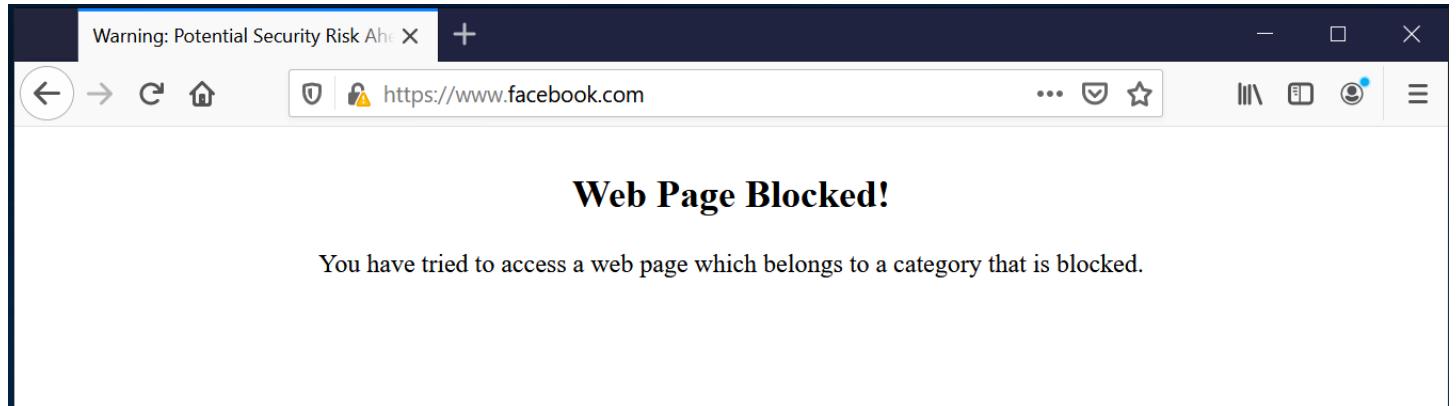
Search

Export

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
LAN (port2) → LAN (port2)	all	all	always	ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	AV default WEB Office_Web_Filter DNS Office_DNS_Filter <input style="color:red; font-size:2em; vertical-align:middle;" type="arrow"/>
LAN (port2) → NYC_to_TLV	all	all	always	ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	IPS default
LAN (port2) → WAN (port1)	all	all	always	ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	SSL Office_To_Internet_Inspection

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.



The screenshot shows a network security log interface. The left sidebar has a 'Favorites' section with 'Firewall Policy', 'Security Events Log' (selected), 'Forward Traffic Log', 'Dashboard', 'Network', 'Policy & Objects', 'Security Profiles', 'VPN', 'User & Authentication', 'WiFi Controller', 'System', 'Security Fabric', and 'Log & Report'. A red circle is on the 'Log & Report' icon. The main area shows a table of logs. A red arrow points from the 'Domain Name' column to the entry for 'star-mini.c10r.facebook.com'. Another red arrow points from the 'Message' column to the text 'Domain was blocked because it is in the domain-filter list' at the bottom right of the table.

Logs							
Date/Time	Event Type	Source	Domain Name	Query Type	Pol	Log Details	
2024/03/01 09:28:47	dns-response	10.104.11.200	star-mini.c10r.facebook.com	AAAA	Tra	Destination 185.89.218.12	
2024/03/01 09:28:47	dns-response	10.104.11.200	star-mini.c10r.facebook.com	A	Tra	Destination Port 53	
2024/03/01 09:04:36	dns-response	10.104.11.200	science-edge-external-prod-7...	A	Tra	Destination Country/Region Ireland	
2024/03/01 09:04:36	dns-response	10.104.11.200	pubsub-edge.twitch.tv	A	Tra	Destination Interface WAN (port1)	
2024/03/01 09:04:36	dns-response	10.104.11.200	passport.twitch.tv	A	Tra	Application Control	
2024/03/01 09:04:36	dns-response	10.104.11.200	irc-ws.chat.twitch.tv	A	Tra	Protocol 17	
2024/03/01 09:04:36	dns-response	10.104.11.200	d1v8493p60f7at.cloudfront....	A	Tra	Data	
2024/03/01 09:04:36	dns-response	10.104.11.200	d186rixkn5rub.acloudfront.N...	A	Tra	Message Domain was blocked because it is in the domain-filter list	
2024/03/01 08:55:37	dns-response	10.104.11.200	ns03.ebaydns.com	A	Tra		
2024/03/01 08:55:33	dns-response	10.104.11.200	ns03.ebaydns.com	A	Tra		

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

The screenshot shows the FortiGate management interface. On the left, a sidebar lists various security profiles: Dashboard, Network, Policy & Objects, Security Profiles (selected), AntiVirus (highlighted with a red underline), Web Filter, Video Filter, DNS Filter, Application Control, Intrusion Prevention, File Filter, SSL/SSH Inspection, and Application Signatures. The main panel is titled "New AntiVirus Profile". It contains the following fields:

- Name: Office_AV_Profile
- Comments: Write a comment... (0/255)
- AntiVirus scan: Block (selected) | Monitor
- Feature set: Flow-based (selected) | Proxy-based
- Inspected Protocols:
 - HTTP: Enabled
 - SMTP: Enabled
 - POP3: Enabled
 - IMAP: Enabled
 - FTP: Enabled
 - CIFS: Enabled

We put this profile on PORT 1

Policy & Objects	Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log
Firewall Policy	+ LAN (port2) → LAN (port2) 1							
IPv4 DoS Policy	+ LAN (port2) → NYC_to_TLV 1							
ZTNA	+ LAN (port2) → WAN (port1) 1							
Authentication Rules	TrafficOut	all	all	always	ALL	✓ ACCEPT	✓ Enabled	AV Office_AV_Profile ← All WEB default DNS Office_DNS_Filter IPS default SSL Office_To_Internet_Inspection
Addresses								
Internet Service Database								
Services								

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

High Security Alert | wildfire.paloaltonetworks.com/publicapi/test/apk

High Security Alert

You are not permitted to download the file "wildfire-test-apk-file.apk" because it is infected with the virus "Android/PaloAlto_Test_Apk_File".

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

Quarantined File Name: [disabled]

Reference URL: http://www.fortinet.com/ve/?vn=Android%2FPaloAlto_Test_Apk_File

wildfire-test-macos-file Failed - Network error

wildfire-test-macos-file Failed - Network error

wildfire-test-apk-file.apk Failed - Network error

New Text Document - Notepad

- APK-https://wildfire.paloaltonetworks.com/publicapi/test/apk
- MacOSX-https://wildfire.paloaltonetworks.com/publicapi/test/macos
- APK-http://wildfire.paloaltonetworks.com/publicapi/test/apk
- MacOSX-http://wildfire.paloaltonetworks.com/publicapi/test/macos

You can also see this in the logs.

Network	Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
Policy & Objects	2024/03/01 06:27:28	10.90.1.10		35.222.124.72 (us-central1.wildfire.paloaltonetw...	HTTP	🚫 Deny (Deny: UTM Blocked)	TrafficOut
VPN	2024/03/01 06:27:21	10.90.1.10		35.222.124.72 (us-central1.wildfire.paloaltonetw...	HTTP	🚫 Deny (Deny: UTM Blocked)	TrafficOut
User & Authentication	2024/03/01 06:26:51	10.90.1.10		35.222.124.72 (us-central1.wildfire.paloaltonetw...	HTTP	🚫 Deny (Deny: UTM Blocked)	TrafficOut
WiFi Controller	2024/03/01 06:26:12	10.90.1.10		35.222.124.72 (us-central1.wildfire.paloaltonetw...	HTTP	🚫 Deny (Deny: UTM Blocked)	TrafficOut

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.

The screenshot shows the FortiGate management interface. On the left, a sidebar menu is open under the 'Security Profiles' section, with 'Intrusion Prevention' selected. The main panel is titled 'New IPS Sensor' and contains the following fields:

- Name:** Office_IPS_Profile
- Comments:** Write a comment... (0/255)
- Block malicious URLs:** A toggle switch is turned on.

Below these settings is a section titled 'IPS Signatures and Filters' with a table header:

	Create New	Edit	Delete
Details	Exempt IPs	Action	Packet Logging
No results			

At the bottom of the main panel, there is a section titled 'Botnet C&C' with a button labeled 'Scan Outgoing Connections to Botnet Sites' followed by three buttons: 'Disable', 'Block' (which is highlighted in green), and 'Monitor'.

Adding a new IPS profile to the policy

The screenshot shows the 'Firewall Policy' section of a network management interface. A red arrow points to the 'IPS' column under the 'Security Profiles' header, highlighting the 'Office_IPS_Profile' entry.

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log
[+] LAN (port2) → [+] LAN (port2)						AV default WEB default IPS Office_IPS_Profile SSL Office_To_Internet_Inspection	
[+] LAN (port2) → [+] WAN (port1)							
TrafficOut	all	all	always	ALL	✓ ACCEPT	Enabled	All
Implicit 1							

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

The connection has timed out

The server at 10.242.1.10 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

We also check the LOGS

The screenshot shows the 'Logs' tab of the F5GATEWAY interface. It displays a table of log entries with columns for Date/Time, Severity, Source, Protocol, User, Action, Count, and Attack Name.

Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
2024/03/01 07:16:32	██████	10.242.1.10	6		dropped		BI00dy.Gang
2024/03/01 07:16:31	██████	10.242.1.10	6		dropped		BI00dy.Gang
2024/03/01 07:16:10	██████	10.242.1.10	6		dropped		BI00dy.Gang
2024/03/01 07:16:10	██████	10.242.1.10	6		dropped		BI00dy.Gang

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

The screenshot shows the FortiGate management interface under the 'Application Control' tab. On the left, a sidebar lists various security profiles: AntiVirus, Web Filter, Video Filter, DNS Filter, Security Profiles (selected), Application Control (highlighted in green), Intrusion Prevention, File Filter, SSL/SSH Inspection, Application Signatures, IPS Signatures, Web Rating Overrides, and Web Profile Overrides. The main pane is titled 'New Application Sensor' and displays a message: '93 Cloud Applications require deep inspection. 0 policies are using this profile.' Below this, the 'Name' field is set to 'Office_Application_Control' and the 'Comments' field is empty (0/255). The 'Categories' section shows a list of application categories with counts: Business (179), Collaboration (293), Game (124), Mobile (3), P2P (85), Remote.Access (91) (highlighted with a red arrow), Storage.Backup (296), Cloud.IT (31), Email (87), General.Interest (241), Network.Service (332), Proxy (106), Social.Media (150), and Update (48).

We also send this profile to our policy.

The screenshot shows the 'Firewall Policy' section of the FortiGate interface. The left sidebar has 'Firewall Policy' selected. The main area displays two policies:

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log
LAN (port2) → LAN (port2)	all	all	always	ALL	ACCEPT	Enabled	All
LAN (port2) → WAN (port1)							

Below the policies is a legend for security profiles:

- AV default (Orange)
- WEB default (Blue)
- APP Office_Application_Control (Green)
- IPS Office_IPS_Profile (Yellow)
- SSL Office_To_Internet_Inspection (Brown)

A red arrow points to the 'All' checkbox in the legend.

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

The screenshot shows a Firefox browser window with a yellow border. The address bar shows a warning icon and the URL https://www.teamviewer.com/en-us/?utm_source=google&utm_medium=cpc&utm_campaign=teamviewer&utm_term=teamviewer. The main content area displays the following message:

Software is Preventing Firefox From Safely Connecting to This Site

www.teamviewer.com is most likely a safe site, but a secure connection could not be established. This issue is caused by **FGTAZRWOQO94G2E4**, which is either software on your computer or your network.

Also check the logs

The screenshot shows the 'Logs' section of the FortiGate interface under 'Log & Report'. The left sidebar has 'Log & Report' selected. The main area shows a table of log entries:

Date/Time	Source	Destination	Application Name	Action	Application User	Appl
2024/03/01 07:35:23	10.242.1.10	104.16.62.16 (www.teamviewer.com)	Teamviewer	Block		
2024/03/01 07:35:23	10.242.1.10	104.16.62.16 (www.teamviewer.com)	Teamviewer	Block		

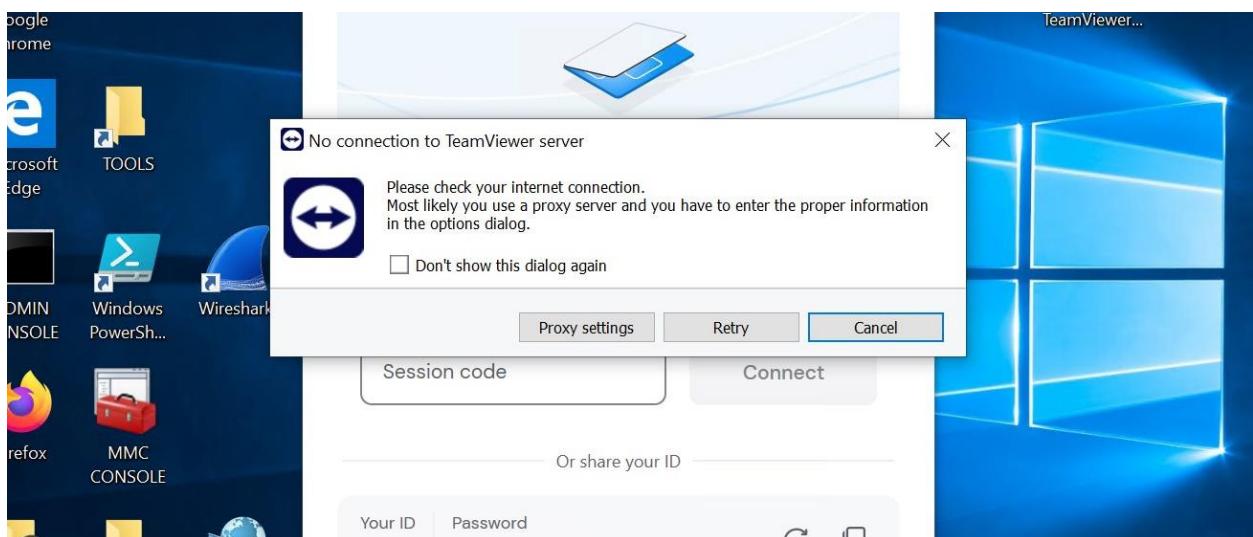
A red arrow points to the 'Block' action in the last row.

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

The screenshot shows the FortiGate Security Profiles interface. On the left, under 'Security Profiles', the 'Application Control' tab is selected. In the center, the 'Web.Client (18)' profile is displayed with 'Network Protocol Enforcement' disabled. Below it, the 'Unknown Applications' profile is shown with a checked checkbox. Under 'Application and Filter Overrides', there is a table listing applications with their details, type (Application), and action (Quarantine). The table data is as follows:

Priority	Details	Type	Action
1	Teamviewer Teamviewer_CallReceive Teamviewer_CallRequest	Application	Quarantine (Expires 2 Day(s))

Let's check this:



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

The screenshot shows the FortiView dashboard under the 'Users & Devices' tab. In the 'Quarantine' section, a green circle indicates 1 total result. The table below shows a single entry for a banned IP address:

Source	Device
App	No results

At the bottom, a table lists the quarantine details:

Details	Device	Source	Expires	Description
Banned IP 1		App	1 day(s) and 23 hour(s)	
10.104.1.10				

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