



MASTERING FORTIGATE

Practical Guide from Basics to Professional
Configuration

<https://www.linkedin.com/in/gitesh-d-aa95a8227/>

Table of Contents

Chapter 1: Introduction to the World of Next-Generation Firewalls (NGFW) and FortiGate.....	3
1.1. What is a Firewall? The Evolution from Traditional Firewalls to NGFW	3
1.2. Introducing Fortinet and FortiGate.....	3
1.3. Why Choose FortiGate?	4
1.4. Who is This Ebook For?.....	4
Chapter 2: Preparation and Initial Setup.....	5
2.1. FortiGate Models	5
2.2. Initial Device Access.....	6
2.3. Setup Wizard.....	7
2.4. Understanding the Main Dashboard.....	7
2.5. Product Registration and Firmware Updates.....	8
Chapter 3: Firewall Objects and Policies (The Core of FortiGate).....	9
3.1. The Logic Behind Firewall Policies.....	9
3.2. Managing Objects.....	10
3.3. Configuring Your First Firewall Policy.....	12
Chapter 4: Securing the Network with Security Profiles (NGFW Features)	16
4.1. The Concept of Security Profiles.....	16
4.2. Configuring Essential Security Features.....	16
4.3. Applying Security Profiles to a Firewall Policy.....	20
Chapter 5: Network Address Translation (NAT) and Virtual IPs (VIPs).....	21
5.2. Configuring SNAT (Internet Access)	22
5.3. Configuring DNAT (Port Forwarding) with a Virtual IP.....	22
Chapter 6: Virtual Private Networks (VPN) for Secure Access.....	25
6.1. Introduction to VPN Concepts	25
6.2. Configuring SSL-VPN (Remote Access).....	25
6.3. Configuring IPsec VPN (Site-to-Site).....	29
Chapter 7: Management, Logging, and Maintenance.....	32

7.1. Users and Authentication.....	32
7.2. Logging and Reporting.....	32
7.3. Backing Up and Restoring Configurations.....	33
7.4. Basic Troubleshooting.....	34
Conclusion: The Next Steps in Your Fortinet Journey.....	35

Chapter 1: Introduction to the World of Next-Generation Firewalls (NGFW) and FortiGate

Welcome to your first step in mastering one of the world's leading network security platforms. In this chapter, we'll build a strong foundation of knowledge before diving into the technical configurations.

1.1. What is a Firewall? The Evolution from Traditional Firewalls to NGFW

Imagine a firewall as a security guard at the main gate of your computer network. Its primary job is to check every "packet" of data trying to enter or leave and decide whether to allow or deny it based on a set of rules.

Traditional firewalls operate at Layer 3 (Network) and Layer 4 (Transport) of the OSI model. They make decisions based on the source IP address, destination IP address, and port number. For example, you could create a rule like: "Allow traffic from the internal network to the internet through port 443 (HTTPS)." This was effective for its time, but it's not enough to handle modern threats.

Cyber threats have evolved. Hackers no longer just attack open ports; they embed malware in downloaded files, exploit application vulnerabilities, or trick users into visiting malicious sites. Traditional firewalls are "blind" to this type of traffic because they don't inspect the content of the data packets themselves.

This is where the Next-Generation Firewall (NGFW) comes in. An NGFW is a smart evolution that not only looks at addresses and ports but also performs a deep inspection of the traffic's content (Deep Packet Inspection). An NGFW can identify specific applications (like Facebook, YouTube, or BitTorrent) regardless of the port they use, and it can scan for viruses, intrusions, and other threats.

1.2. Introducing Fortinet and FortiGate

Fortinet is a global leader in broad, integrated, and automated cybersecurity solutions. Their flagship product is FortiGate, a highly popular NGFW platform known for its high performance and comprehensive security features.

However, Fortinet's strength doesn't stop at the FortiGate. They have a concept called the Fortinet Security Fabric. Imagine this as a security ecosystem where various Fortinet products (like FortiAnalyzer for logging, FortiSwitch for switching, and FortiAP for wireless) can communicate and work together intelligently. The FortiGate acts as the core of this Security Fabric, providing centralized visibility and control over your entire security infrastructure.

1.3. Why Choose FortiGate?

There are three main reasons why many organizations, from small businesses to large enterprises, choose FortiGate:

- **High Performance:** FortiGate uses special processors called SPUs (Security Processing Units) to speed up the security inspection process. This means you can enable many security features without a significant drop in network performance, which is a common issue with other NGFWs.
- **Integrated Security:** With a FortiGate, you get various security functions in one device: firewall, antivirus, web filter, IPS, application control, VPN, and more. This simplifies your network architecture and reduces costs.
- **Ease of Management:** The FortiGate web interface (GUI) is designed to be intuitive and easy to use, even for new administrators. Concepts like structured objects and policies make managing rules more efficient.

1.4. Who is This Ebook For?

This ebook is designed for:

- **Network and System Administrators:** Who want to implement or manage FortiGate in their work environment.

- IT and Cybersecurity Students: Who want to learn practical, in-demand industry skills.
- Security Practitioners: Who want to switch to or deepen their knowledge of the Fortinet platform.
- Anyone interested in network security and wanting to understand how modern NGFWs work in a practical way.

After completing this ebook, you will be able to perform initial configurations, create secure firewall policies, enable essential NGFW features, build VPN connections, and perform basic management on a FortiGate device.

Let's get started!

Chapter 2: Preparation and Initial Setup

In this chapter, we'll turn on the FortiGate device for the first time and perform a series of crucial initial configurations.

2.1. FortiGate Models

FortiGate is available in two main forms:

- **Hardware Appliance:** This is a physical device, ranging from the 40F series for small offices/branches to the 7000F series for large data centers. This hardware comes with physical network ports and SPUs for maximum performance.
- **Virtual Machine (VM):** FortiGate can also run as a virtual machine on platforms like VMware ESXi, Microsoft Hyper-V, or in the cloud (AWS, Azure). This offers flexibility, but its performance depends on the host server's resources.

In this ebook, all configuration guides apply to both models because their operating system (FortiOS) is the same.

2.2. Initial Device Access

When you take a new FortiGate out of the box, there are two main ways to access it:

1. Via the GUI (The Most Common Method):

- By default, the FortiGate's internal port (usually labeled "internal" or "port1") has the IP address 192.168.1.99.
- Connect your laptop to this port using an Ethernet cable.
- Set your laptop's IP address to a static address in the same subnet, for example, 192.168.1.100 with a subnet mask of 255.255.255.0.
- Open a web browser (Chrome/Firefox) and navigate to <https://192.168.1.99>.
- You will see a security certificate warning; click "Proceed" or "Advanced" to continue.
- On the login page, use the username admin and leave the password blank.
- The FortiGate will immediately prompt you to create a new, strong password. Do this to secure the device.

2. Via Console Cable (CLI):

- Connect a console cable (usually included) from the FortiGate's console port to your laptop's serial/USB port.
- Use a terminal application like PuTTY or SecureCRT with the following settings: Baud Rate 9600, Data bits 8, Parity None, Stop bits 1.
- Press Enter a few times, and you will see the login prompt. Use the same credentials as above (admin/no password).

2.3. Setup Wizard

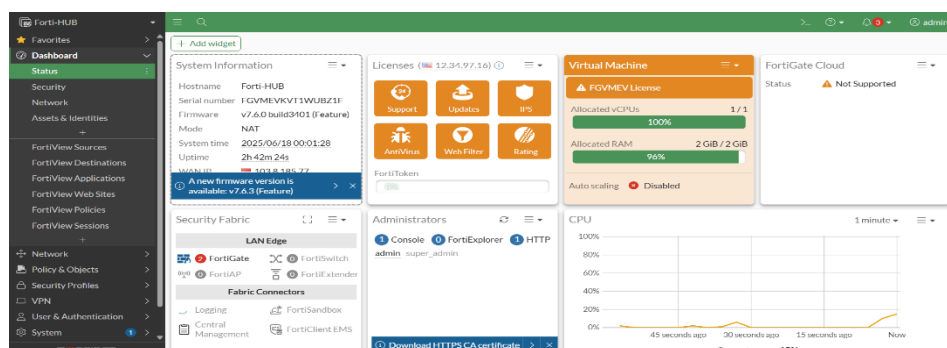
After your first login, the easiest way to perform a basic configuration is with the Setup Wizard. You will usually see this option on the Dashboard. If not, you can find it in the System > Wizards menu. This wizard will guide you through:

- Admin Settings: Changing the admin password (if you haven't already).
- Network Settings: Configuring the IP addresses for the WAN port (connected to the internet) and the LAN port (internal network), as well as DNS servers.
- Registration: Entering your FortiCloud account credentials to register the device.

2.4. Understanding the Main Dashboard

The Dashboard is your main control center. After logging in, take a moment to familiarize yourself with this interface. Some important widgets you will use often are:

- System Information: Displays the device model, FortiOS version, uptime, and license status.
- Security Fabric: Shows the connectivity status with other Fortinet devices.
- FortiView: Provides real-time visualizations of sessions, sources, destinations, and applications passing through the firewall. Very useful for troubleshooting.
- Administrators: Shows who is currently logged into the device.
- Picture for Fortigate GUI Dashboard :

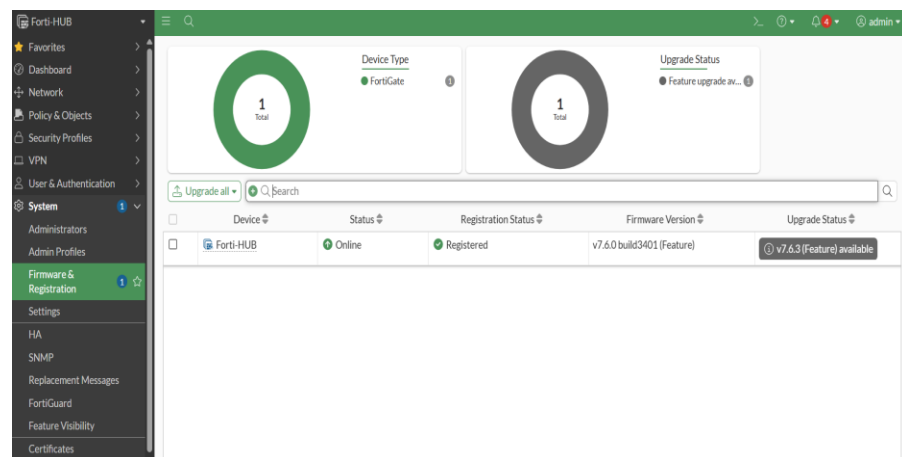


2.5. Product Registration and Firmware Updates

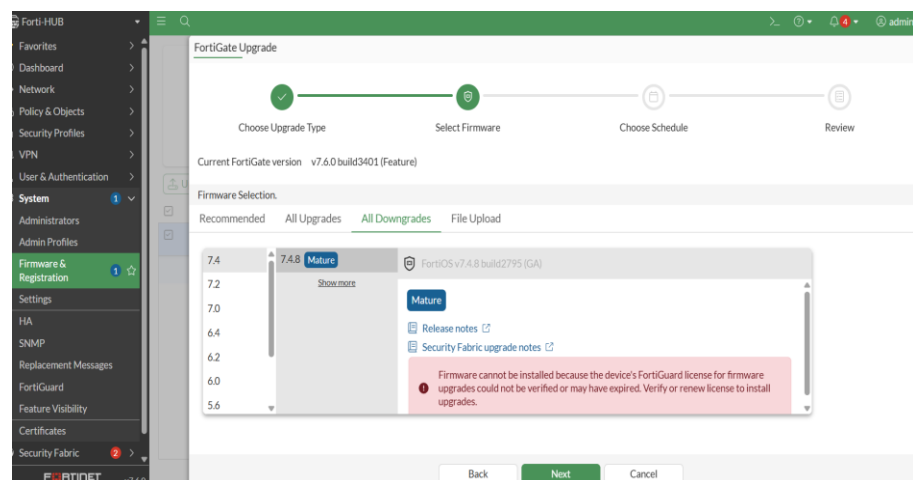
This step is critically important. Without registration, security features like Antivirus, IPS, and Web Filter will not get updates and will not function.

- **Registration:** In the System Information widget, you will see the license status. Click the "Register" link and follow the instructions to link the device to your FortiCare/FortiCloud account. Once successful, the license status will turn valid.
- **Firmware Update:** Security is an ongoing process. Fortinet regularly releases firmware updates to add new features and patch vulnerabilities.

1. Navigate to System > Firmware.



2. The FortiGate will display the current firmware version and the latest available version.



3. Important: Before updating, always read the Release Notes. Sometimes there are significant changes or potential issues.
4. Always back up your configuration before performing an update (covered in Chapter 7).
5. Click the "Upgrade" button and upload the firmware file you have downloaded from the Fortinet support site. The device will reboot, and this process will take a few minutes.

After completing the steps in this chapter, your FortiGate is now secure, up-to-date, and ready for further configuration.

Chapter 3: Firewall Objects and Policies (The Core of FortiGate)

This is the heart of every firewall. In this chapter, we'll learn how the FortiGate makes decisions and how we can control it through Firewall Policies.

3.1. The Logic Behind Firewall Policies

Think of a firewall policy as a series of "if-then" rules that the FortiGate reads from top to bottom. When a data packet arrives at the FortiGate, it will match the packet against each policy in order. As soon as a matching policy is found, the FortiGate applies the action from that policy and stops processing further rules.

Each policy consists of several key parameters:

- Incoming Interface: Where is the traffic coming from? (e.g., LAN port).
- Outgoing Interface: Where is the traffic going? (e.g., WAN port).
- Source: Who or what is starting the connection? (e.g., all IPs on the internal network).
- Destination: Who or what is the target of the connection? (e.g., all addresses on the internet).
- Service: What type of traffic is it? (e.g., HTTPS, DNS).

- Action: What should be done with this traffic? (ACCEPT or DENY).

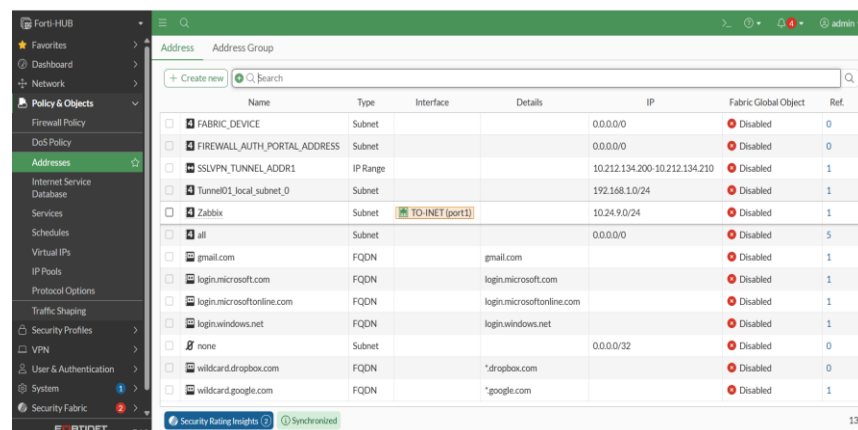
If no policy matches, the traffic will be rejected by the final, invisible rule, which is the Implicit Deny.

3.2. Managing Objects

To create clean and manageable policies, FortiGate uses the concept of Objects. Instead of typing an IP address repeatedly, you create an object that represents it.

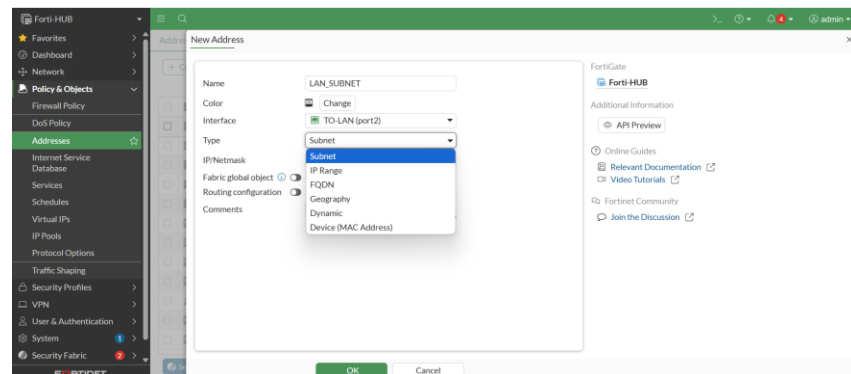
Navigate to Policy & Objects > Addresses to get started.

- Addresses: This is a representation of an IP address.
 - Click Create New > Address.



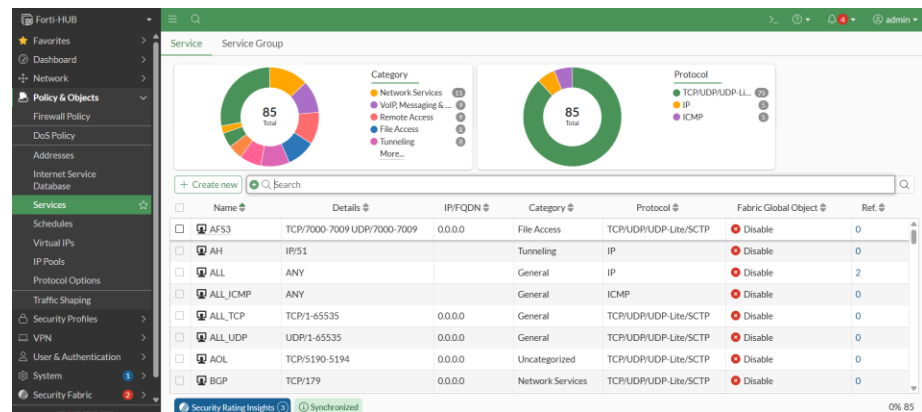
Name	Type	Interface	Details	IP	Fabric Global Object	Ref.
FABRIC_DEVICE	Subnet			0.0.0.0/0	Disabled	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet			0.0.0.0/0	Disabled	0
SSLVPN_TUNNEL_ADDR1	IP Range			10.212.134.200-10.212.134.210	Disabled	1
Tunnel01_local_subnet_0	Subnet			192.168.1.0/24	Disabled	1
Zabbix	Subnet	TO-INET (port1)		10.24.9.0/24	Disabled	1
all	Subnet			0.0.0.0/0	Disabled	5
gmail.com	FQDN		gmail.com		Disabled	1
login.microsoft.com	FQDN		login.microsoft.com		Disabled	1
login.microsoftonline.com	FQDN		login.microsoftonline.com		Disabled	1
login.windows.net	FQDN		login.windows.net		Disabled	1
none	Subnet			0.0.0.0/32	Disabled	0
wildcard.dropbox.com	FQDN		*.dropbox.com		Disabled	0
wildcard.google.com	FQDN		*.google.com		Disabled	1

- Name: Give it a descriptive name (e.g., LAN_Subnet or WebServer_Internal_IP).

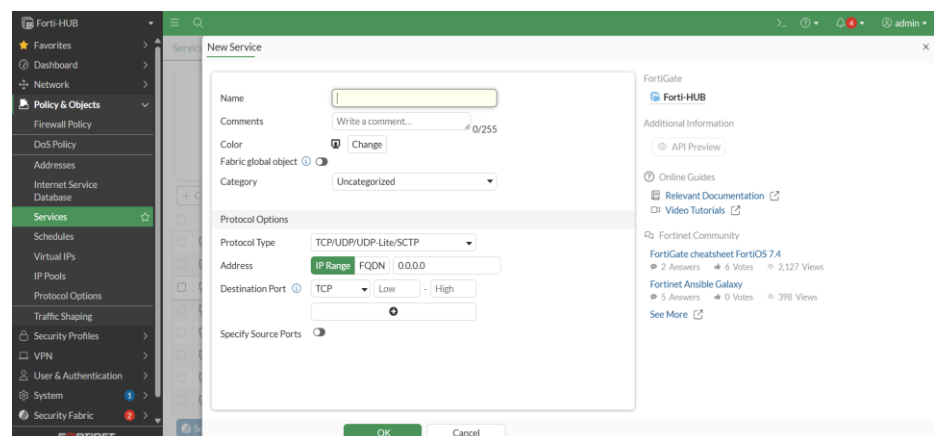


- Type: Choose the type. The most common are:

- Subnet: To define an entire network (e.g., 192.168.1.0/24).
 - IP/Netmask: Same as subnet.
 - FQDN: To define a domain name (e.g., office365.com). The FortiGate will automatically resolve the IP behind it.
 - IP Range: For a range of IPs (e.g., 192.168.1.100-192.168.1.150).
- Services: This represents a port or protocol. Navigate to Policy & Objects > Services.
 - FortiGate already has many built-in services (HTTP, HTTPS, DNS, etc.).

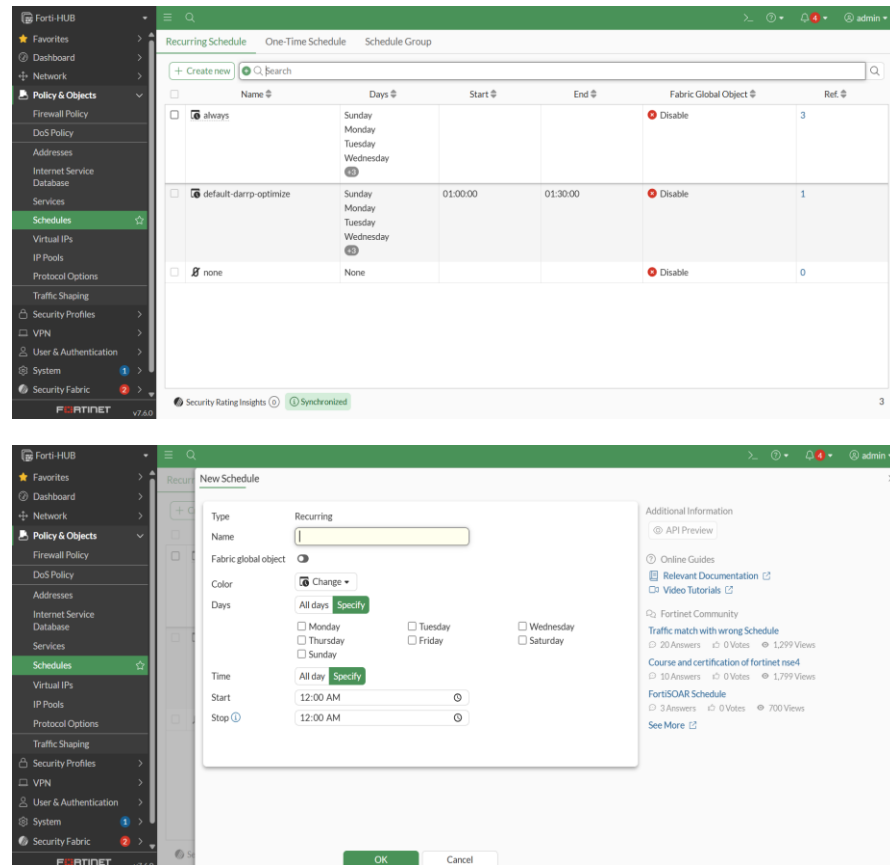


- However, if you have an application with a custom port, click Create New > Service.



- Give it a name (e.g., CustomApp_TCP_8080), select the protocol (TCP/UDP/SCTP), and enter the destination port.
- Schedules: This represents a time. Navigate to Policy & Objects > Schedules.

- Click Create New > Schedule to define a specific time, for example, Office_Hours which is active from Monday-Friday, 9 AM to 5 PM. This can be used in a policy to restrict access to only those hours.



3.3. Configuring Your First Firewall Policy

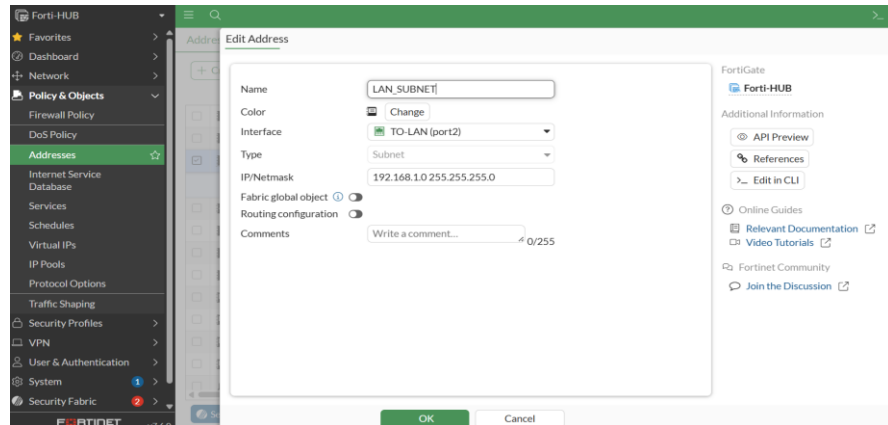
Let's apply all these concepts in a very common scenario.

Case Study: Allowing all users on the internal network (LAN) to access the internet (WAN).

Step-by-Step:

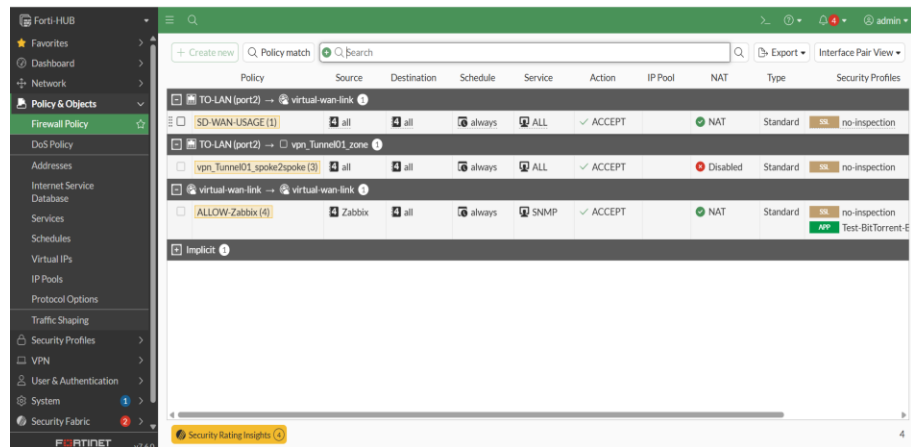
1. Create an Address Object for the LAN Network (if it doesn't exist):
 - Navigate to Policy & Objects > Addresses.
 - Click Create New > Address.

- Name: LAN_Network
- Type: Subnet
- Subnet / IP Range: 192.168.1.0/24 (adjust to your network).
- Click OK.

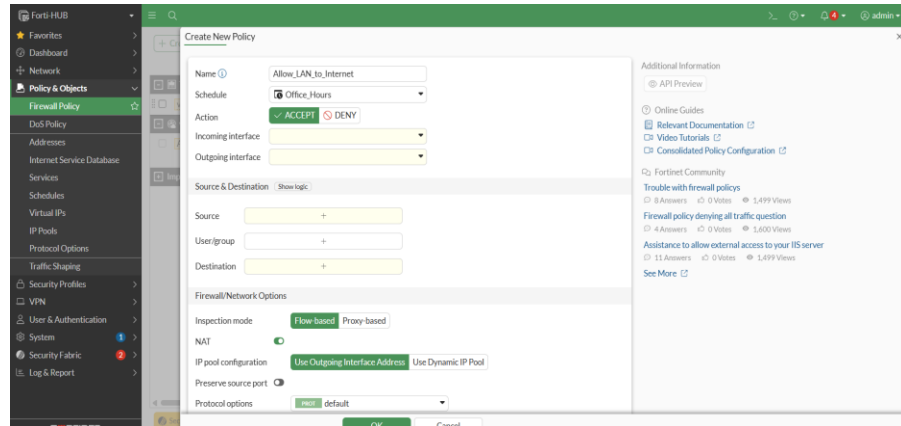


2. Create the Firewall Policy:

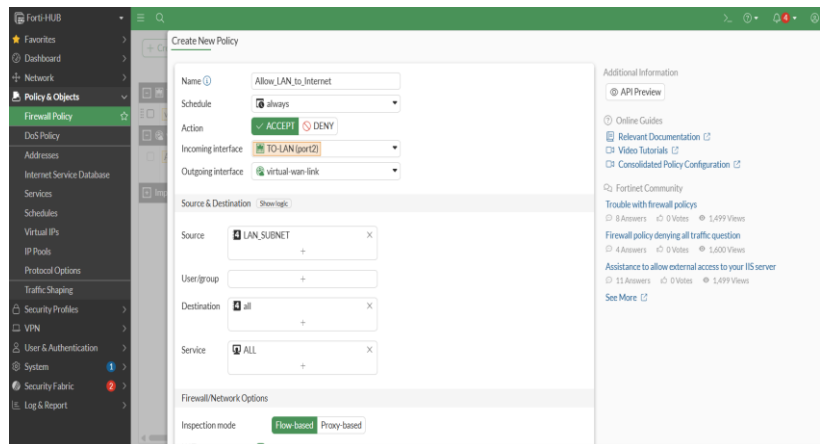
- Navigate to Policy & Objects > Firewall Policy.



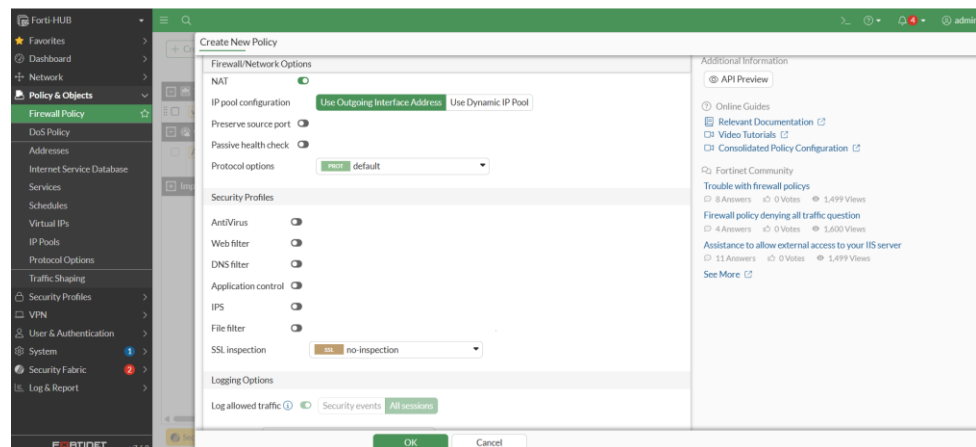
- Click the Create New button.



- A panel will open to create a new policy. Fill it out as follows:
 - Name: Allow_LAN_to_Internet
 - Incoming Interface: Select your LAN port (e.g., port2 or internal).
 - Outgoing Interface: Select your WAN port (e.g., port1 or wan1).
 - Source: Click the + sign and select the LAN_Network object you just created. You can also add the all object if you're not sure yet.
 - Destination: Click the + sign and select the all object. This represents all addresses on the internet.
 - Service: Click the + sign and select ALL. For more security, you can choose specific services like HTTP, HTTPS, and DNS.
 - Action: Choose ACCEPT.



- Make sure NAT is enabled! Scroll down and ensure the NAT toggle is in the ON position and is using the Use Outgoing Interface Address option. This is important so that devices on your internal network can use the FortiGate's public IP to communicate with the internet. (More details in Chapter 5).
- Enable Logging: In the Logging Options section, enable Log Allowed Traffic and select All Sessions. This is very important for monitoring and troubleshooting.
- Click OK.



Your new policy is now active. Try opening a browser from a computer on the LAN, and you should be able to access the internet.

Best Practices

- Naming: Always use clear and consistent names for objects and policies (e.g., Allow_Marketing_to_Web, Deny_Guest_to_Internal).
- Description: Use the comment field in policies to explain their purpose. This will be very helpful in the future.
- Principle of Least Privilege: Don't use all or ANY if it's not necessary. The more specific your rules are, the more secure your network is. Start with strict rules, then open up access as needed.
- Policy Order: Place the most specific policies at the top. For example, a policy to block access from a specific user must be above a general policy that allows access.

Chapter 4: Securing the Network with Security Profiles (NGFW Features)

Once basic traffic is allowed by a Firewall Policy, it's time to enable the intelligence of the NGFW. Security Profiles are an additional layer of security that inspects the content of allowed traffic.

4.1. The Concept of Security Profiles

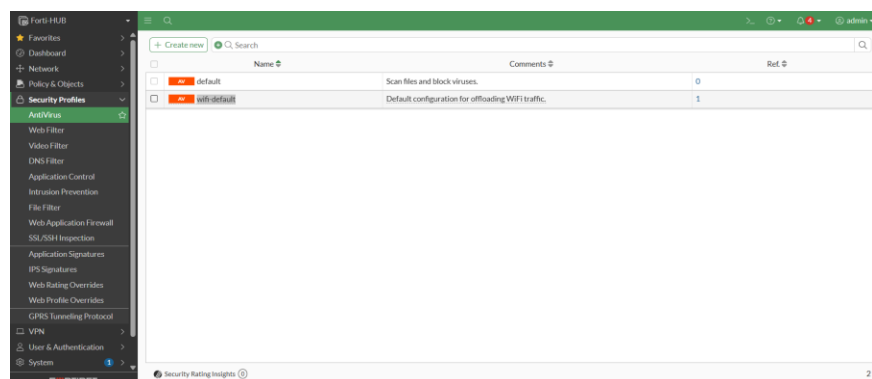
Imagine a Firewall Policy as a gatekeeper who checks an ID card (IP and port). If the ID is valid, the person is allowed in. However, Security Profiles are a second security check inside the gate, like a metal detector or an x-ray scanner, that checks the person's belongings for dangerous items.

Each security profile (Antivirus, Web Filter, etc.) can be configured independently and then "attached" to one or more Firewall Policies.

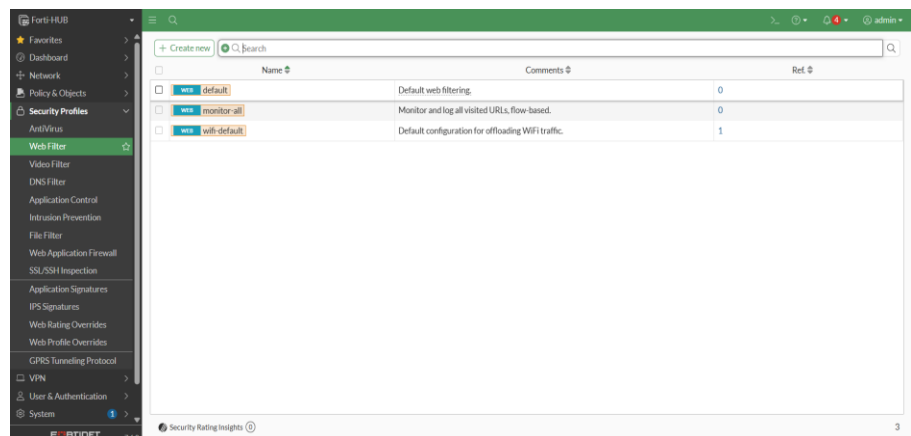
4.2. Configuring Essential Security Features

Let's configure the most common security profiles. Navigate to Security Profiles in the left-hand menu.

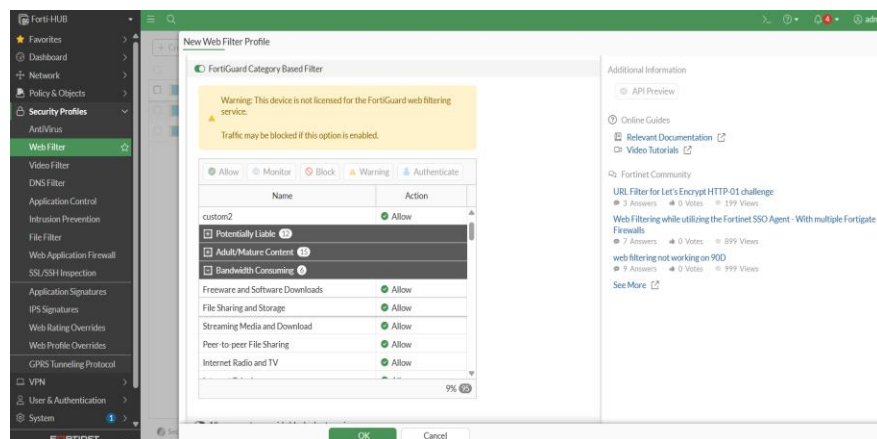
- Antivirus (AV):
 1. Go to Security Profiles > AntiVirus.



2. You will see a default profile. You can edit it or create a new one by clicking Create New.
 3. Inside the profile, make sure Scan Files is enabled. You can choose which protocols you want to scan (HTTP, FTP, email, etc.).
 4. For starters, using the default option is good enough.
- Web Filter:
 1. Go to Security Profiles > Web Filter.



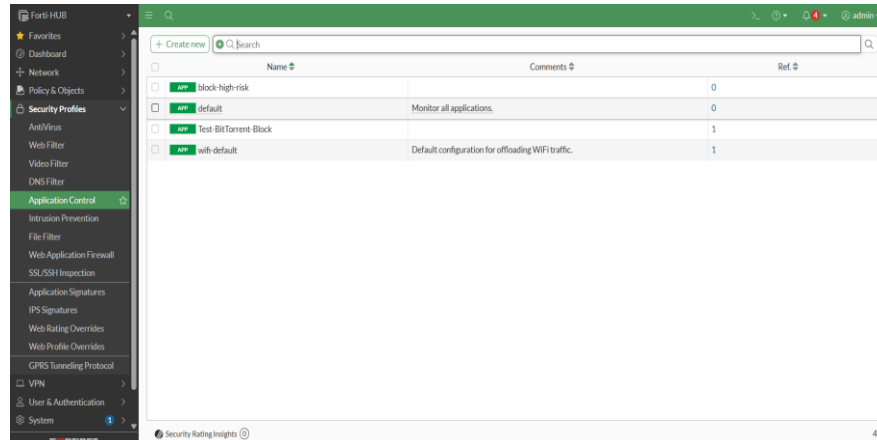
2. Edit the default profile or create a new one.
3. This is a very powerful feature. You will see a list of FortiGuard Category Based Filters. Here you can block categories of websites.
4. Example: Find the "Bandwidth Consuming" category and right-click > Block. This will block video streaming sites. Find the "Malicious Websites" category and make sure it is set to Block.



5. You can also perform a Static URL Filter to block or allow specific domains.

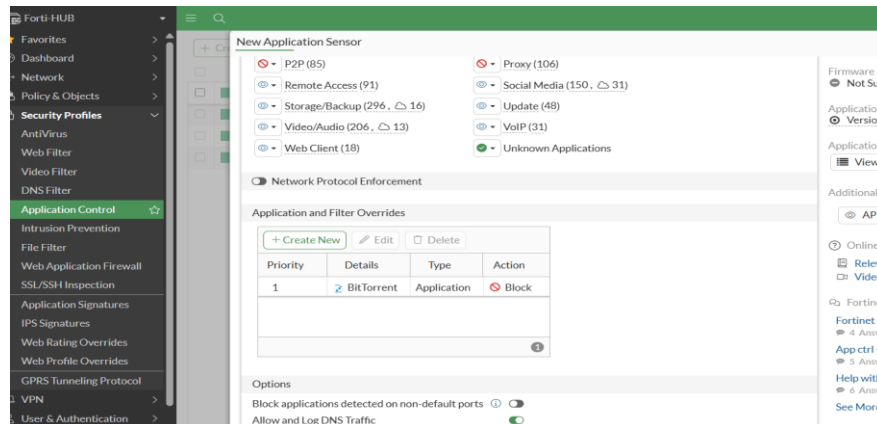
- Application Control:

1. Go to Security Profiles > Application Control.



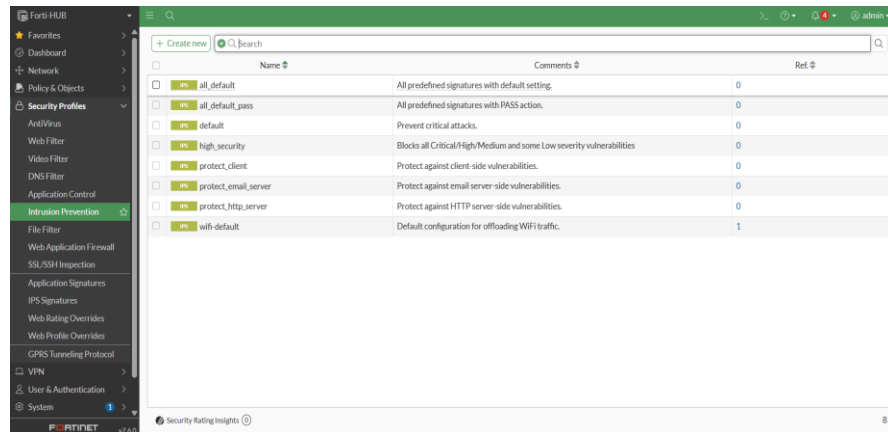
2. This feature lets you control applications, not just websites.

3. Example: Under Application and Filter Overrides, click Create New. In the Application field, type "BitTorrent". Select the application, then set the Action to Block. This will prevent anyone from using the BitTorrent application on your network.



- Intrusion Prevention System (IPS):

1. Go to Security Profiles > Intrusion Prevention.



2. IPS protects the network from attacks that try to exploit software vulnerabilities.
 3. Edit the default profile. Click Create New under IPS Signatures and Filters.
 4. The easiest way is to use the built-in filters. Add filters with the Severity set to critical, high, and medium, with the Action set to Block. This will automatically block thousands of known attacks.
- DNS Filter:

1. Go to Security Profiles > DNS Filter.

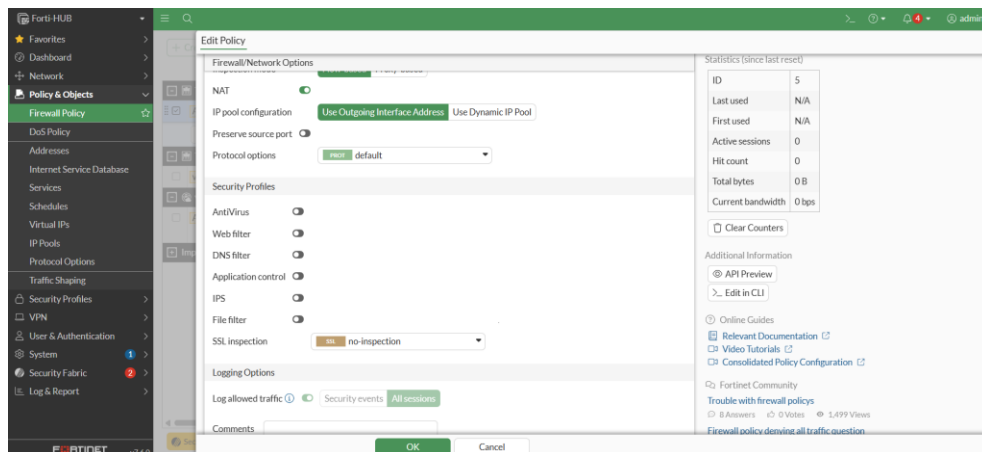


2. This feature blocks DNS requests to known malicious domains or domains in unwanted categories, even before a TCP connection is made.
3. Enable blocking for the "Malicious Websites" category and other relevant categories.

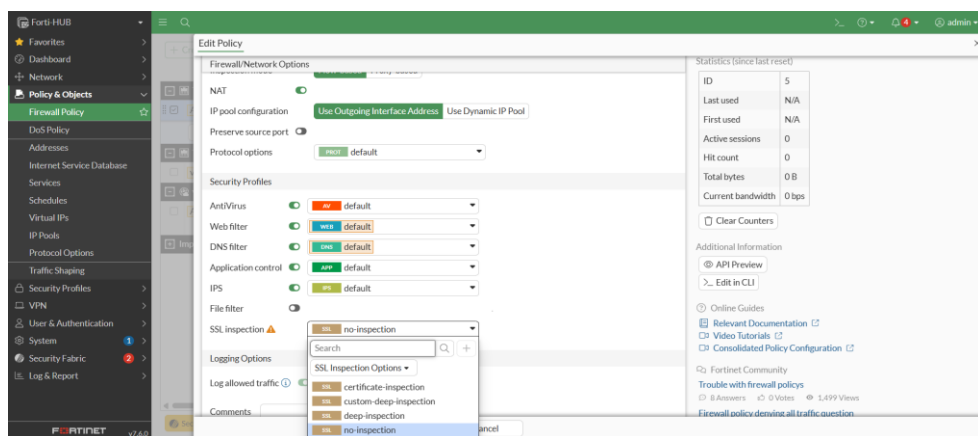
4.3. Applying Security Profiles to a Firewall Policy

Once your security profiles are ready, it's time to activate them.

1. Go back to Policy & Objects > Firewall Policy.
2. Edit the policy we created earlier (Allow_LAN_to_Internet).
3. Scroll down to the Security Profiles section.



4. You will see a toggle for each type of profile. Enable those toggles.
5. Select the profile you want to use from the dropdown menu (e.g., select the default profile for Antivirus, Web Filter, IPS, Application Control, and DNS Filter).



6. Make sure SSL Inspection is set. This is an advanced topic, but for now, choose certificate-inspection. This allows the FortiGate to see the domain

name inside HTTPS traffic, which is necessary for the Web Filter and Application Control to work properly for encrypted sites.

7. Click OK.

Now, all traffic that matches the Allow_LAN_to_Internet policy will not only be allowed but will also be deeply inspected by all the security profiles you enabled. You have transformed your firewall from a simple traffic cop into a sophisticated defense system.

Chapter 5: Network Address Translation (NAT) and Virtual IPs (VIPs)

On the internet, public IP addresses are a limited and valuable resource. The majority of devices on an internal network (LAN) use private IP addresses (like 192.168.x.x) that cannot be routed on the internet. This chapter explains how the FortiGate bridges these two worlds using NAT.

5.1. What is NAT? The Concepts of SNAT and DNAT

Network Address Translation (NAT) is the process of modifying IP address information in data packet headers while in transit through a router or firewall. There are two main types:

- Source NAT (SNAT): Changes a private *source* IP address to a public IP address. This is used when internal users want to access the internet. All requests from the LAN will appear to come from the single public IP address of the FortiGate. This is what allows many devices to share one internet connection.
- Destination NAT (DNAT): Changes a public *destination* IP address to a private IP address. This is used when someone from the internet wants to access a server (like a web server) that is inside your LAN. The FortiGate receives the request on its public IP and forwards it to the correct internal server. In FortiGate, this is implemented using a Virtual IP (VIP).

5.2. Configuring SNAT (Internet Access)

The good news is, you've already done this! When we created the firewall policy in Chapter 3 and enabled the NAT toggle, we were actually configuring SNAT. The Use Outgoing Interface Address option tells the FortiGate to automatically use the IP address of the Outgoing Interface (in our case, the WAN port) as the source address for all outgoing traffic. This is the most common form of SNAT and is known as Overload or PAT (Port Address Translation).

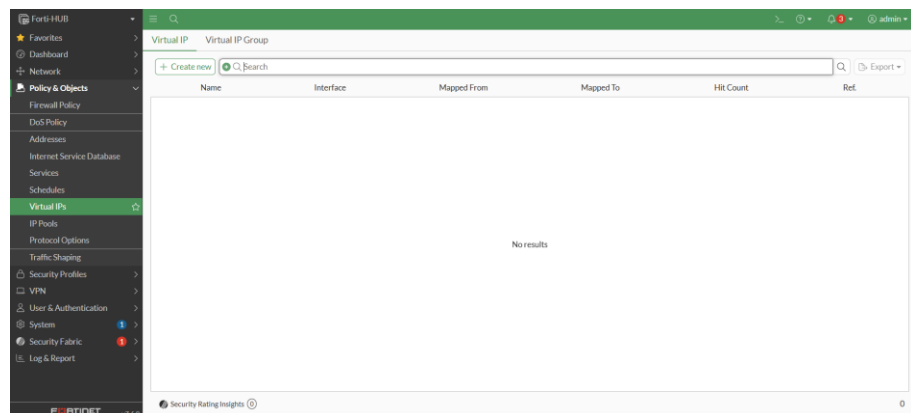
5.3. Configuring DNAT (Port Forwarding) with a Virtual IP

Let's tackle a more interesting scenario.

Case Study: You have a CCTV server on your internal network with the IP 192.168.1.50. You want to be able to view the CCTV footage from anywhere on the internet, using port 8080.

Step-by-Step:

1. Create a Virtual IP (VIP) Object:
 - Navigate to Policy & Objects > Virtual IPs.



- Click Create New > Virtual IP.
- Name: CCTV_Server_VIP

- External IP Address/Range: Enter your FortiGate's public IP address. If you're unsure, select the object that represents your WAN interface (e.g., wan1).
- Mapped IP Address/Range: Enter the private IP address of your CCTV server, which is 192.168.1.50.
- Enable Port Forwarding.
- Protocol: TCP
- External Service Port: 8080 (The port you will use to access it from the internet).
- Map to Port: 80 (The original port where the CCTV service is running on the internal server. Adjust if different).

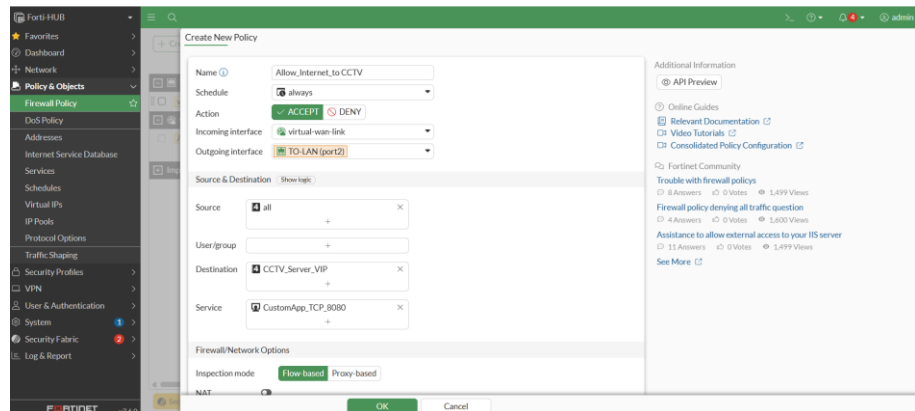
The screenshot shows the FortiGate web interface for configuring a new virtual IP. The sidebar on the left lists various configuration categories, with 'Virtual IPs' highlighted. The main panel is titled 'New Virtual IP' and contains several input fields and checkboxes. The 'Name' field is set to 'CCTV_Server'. The 'Network' section shows the interface as 'TO-LAN (port2)' and the type as 'Static NAT' with 'FQDN' selected. The 'External IP address/range' is '10.24.9.16' and the 'Map to' field shows 'IPv4 address/range' as '192.168.1.50'. Under 'Optional Filters', 'Port Forwarding' is enabled, and the 'Protocol' is set to 'TCP'. The 'Port Mapping Type' is 'One to one', the 'External service port' is '8080', and the 'Map to IPv4 port' is '80'. At the bottom, there are 'OK' and 'Cancel' buttons. On the right side, there's a 'FortiGate' section with 'Forti-HUB' and a 'Statistics (since last reset)' table.

- Click OK.

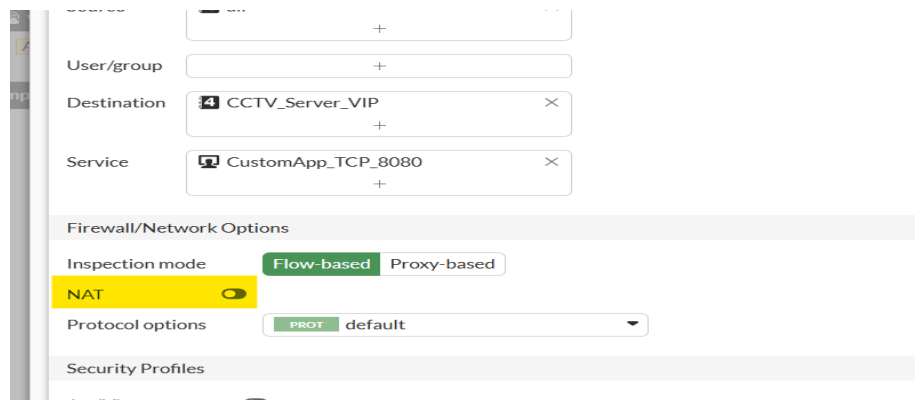
2. Create a Firewall Policy to Allow Access:

- Now we need to create a rule that explicitly allows traffic from the internet to our server.
- Navigate to Policy & Objects > Firewall Policy.
- Click Create New.
- Name: Allow_Internet_to_CCTV
- Incoming Interface: wan1 (the port facing the internet).

- Outgoing Interface: lan (the port where the CCTV server is connected).
- Source: all (since you want to access it from anywhere).
- Destination: Select the VIP object you just created, CCTV_Server_VIP.
- Service: Select the appropriate service, for example, TCP_8080 or create a custom service if needed. To be safe, you can choose the service that matches the port you are forwarding.
- Action: ACCEPT.



- **IMPORTANT:** Make sure the NAT toggle is in the OFF position. We don't want to perform SNAT on this traffic because we are already doing DNAT using the VIP.



- Click OK.

Now, if you open a browser from an external network and type `http://<Your-Public-IP>:8080`, the FortiGate will receive the request, translate it, and forward it to your CCTV server at 192.168.1.50 on port 80.

Best Practices

- Port Forwarding: Only open the ports you absolutely need. Never place an internal server in a DMZ or forward all ports unless it's absolutely necessary.
- Extra Security: For policies that allow inbound access (DNAT), always apply Security Profiles (especially IPS) to protect your internal server from attacks.
- Limited Source: If you know which IPs you will be accessing the server from (e.g., from your head office), restrict the Source field in your DNAT policy to those IP addresses instead of using all.

Chapter 6: Virtual Private Networks (VPN) for Secure Access

A VPN creates a secure, encrypted "tunnel" through a public network like the internet. This is a fundamental technology for remote work and connecting branch offices.

6.1. Introduction to VPN Concepts

There are two main types of VPN implementations in FortiGate:

- SSL-VPN (Remote Access): Perfect for individual users (like employees working from home) who need to access the office network from their laptops or mobile devices. They only need a browser or a lightweight client application (FortiClient).
- IPsec VPN (Site-to-Site): Used to permanently connect two office networks, as if they were in the same location. This typically connects two firewalls (for example, a FortiGate in Jakarta and a FortiGate in Surabaya).

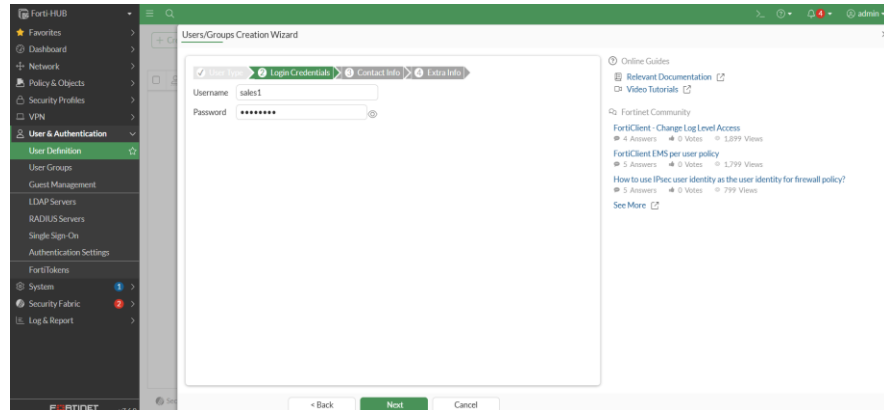
6.2. Configuring SSL-VPN (Remote Access)

Case Study: Allowing a traveling sales team to connect to the office network and access a file server.

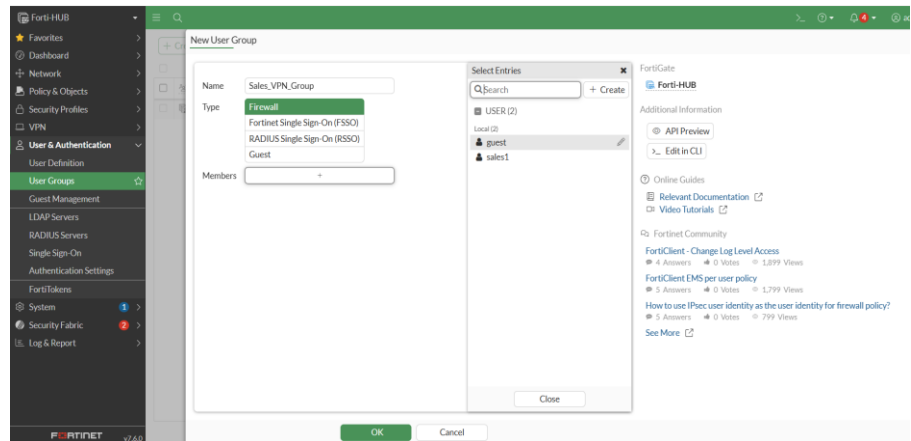
Step-by-Step:

1. Create Users and a User Group:

- Navigate to User & Authentication > User Definition to create user accounts for each member of the sales team.

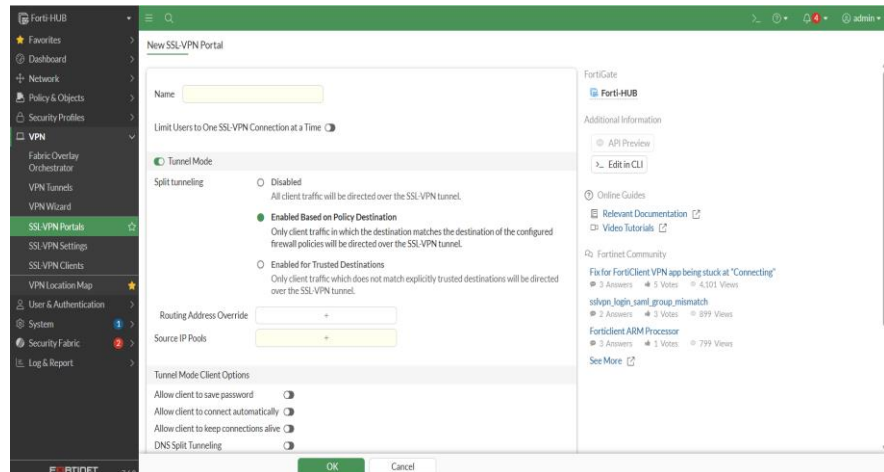


- Navigate to User & Authentication > User Groups and create a new group called Sales_VPN_Group, then add all the sales users to it.



2. Configure the SSL-VPN Portal:

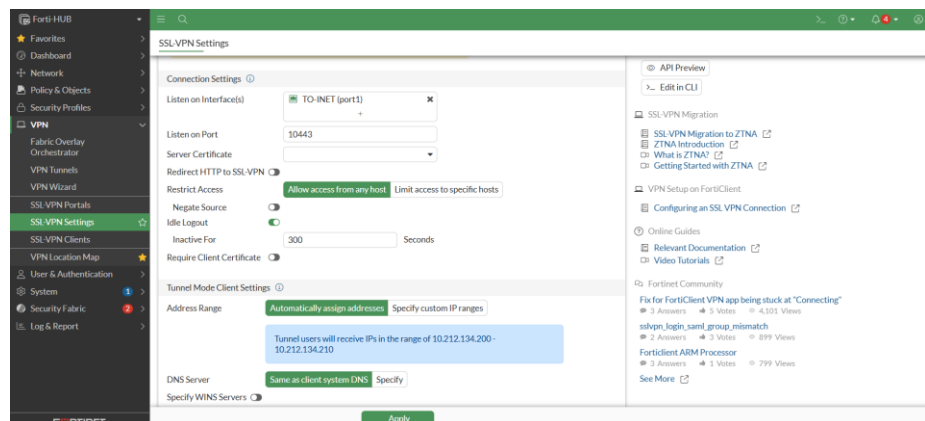
- Navigate to VPN > SSL-VPN Portals. A portal defines what users can access after they connect.



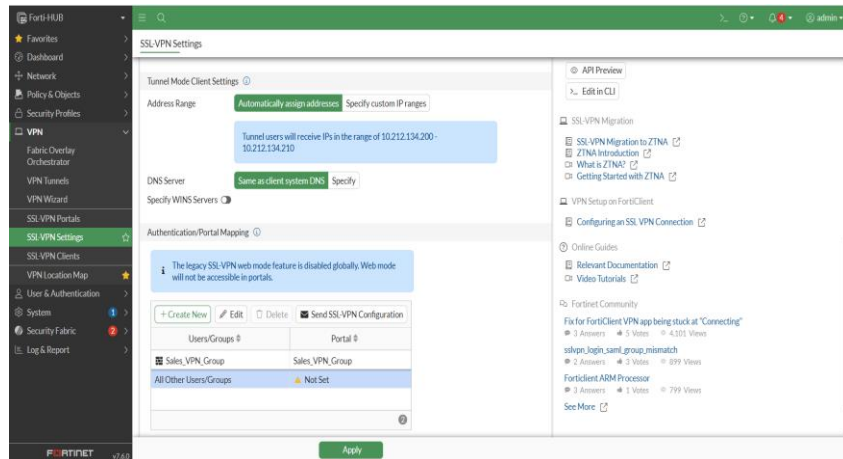
- You can edit the full-access portal or create a new one. Make sure Tunnel Mode is enabled.

3. Configure SSL-VPN Settings:

- Navigate to VPN > SSL-VPN Settings.
- Listen on Interface(s): Select your WAN interface (wan1).
- Listen on Port: The default port is 443. If this port is already in use for something else, you can change it (e.g., to 10443).

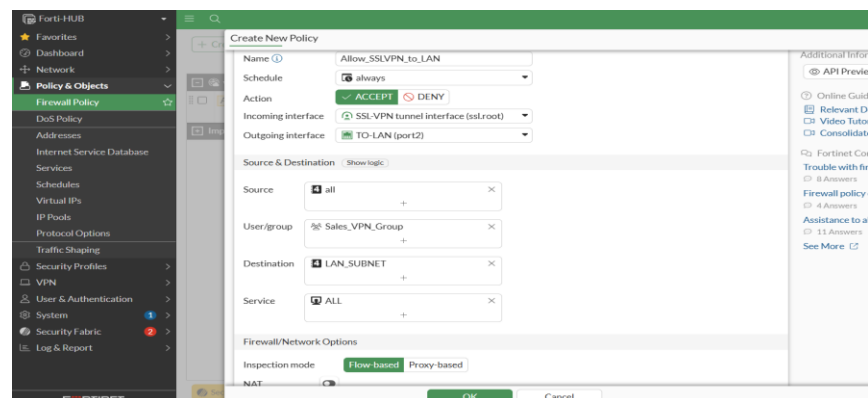


- Under Authentication/Portal Mapping, click Create New.
 - User Group: Select Sales_VPN_Group.
 - Portal: Select the full-access portal.
 - Click OK.



4. Create a Firewall Policy for VPN Access:

- Navigate to Policy & Objects > Firewall Policy.
- Click Create New.
- Name: Allow_SSLVPN_to_LAN
- Incoming Interface: Select the virtual interface ssl.root. This is a special interface for SSL-VPN traffic.
- Outgoing Interface: Select your LAN interface (lan).
- Source: Select the Sales_VPN_Group user group and the all object.
- Destination: Select the address object that represents your LAN (LAN_Network).
- Service: ALL or the specific services needed.
- Action: ACCEPT.
- Make sure NAT is in the OFF position.



- Click OK.

5. Connecting from the Client:

- Users can now download and install FortiClient VPN (the free version is sufficient).
- In FortiClient, they will create a new connection, enter your FortiGate's public IP address, and log in with their username and password. Once connected, they will get an IP address from the SSL-VPN range and can access resources on the LAN according to the firewall rules you created.

6.3. Configuring IPsec VPN (Site-to-Site)

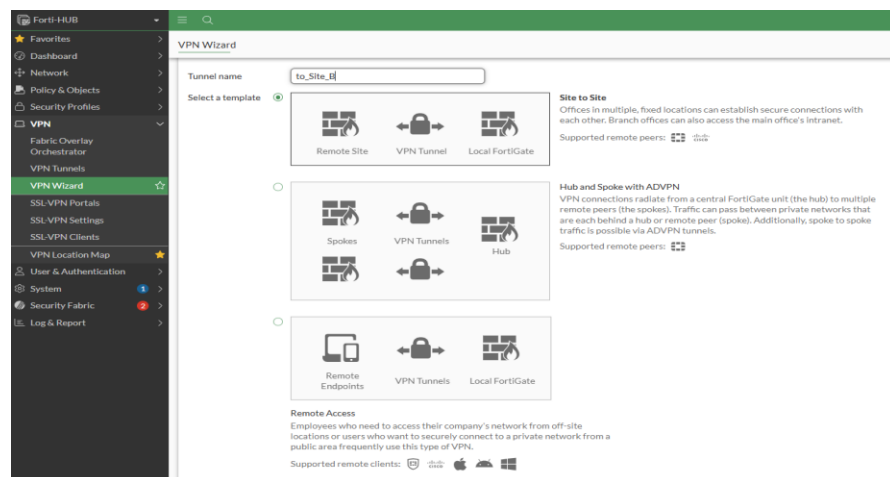
Case Study: Securely connecting a head office (Site A) with a branch office (Site B) over the internet.

The easiest way to do this is by using the VPN Wizard.

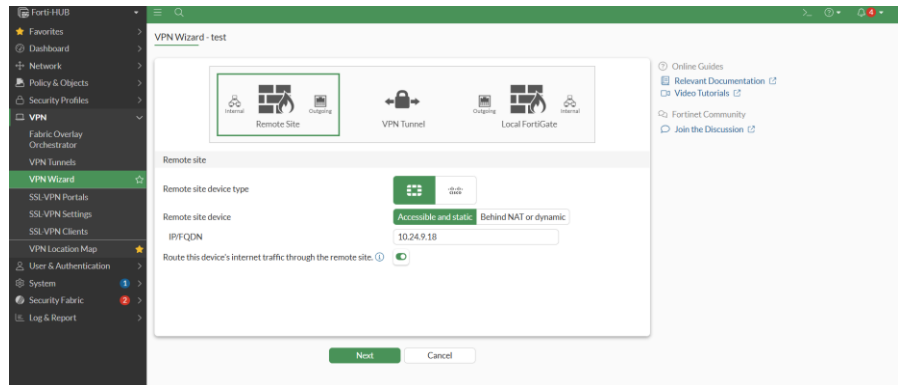
Step-by-Step (performed on both FortiGates):

1. Run the VPN Wizard on Site A:

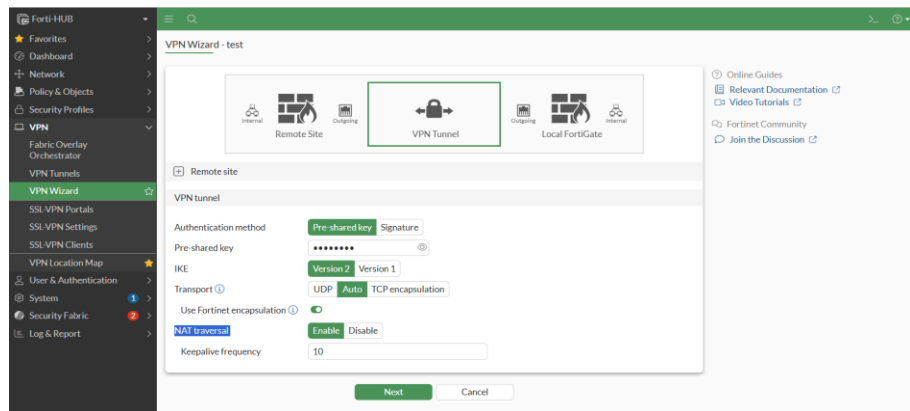
- Navigate to VPN > IPsec Wizard.
- Name: to_Site_B
- Template Type: Choose Site to Site.



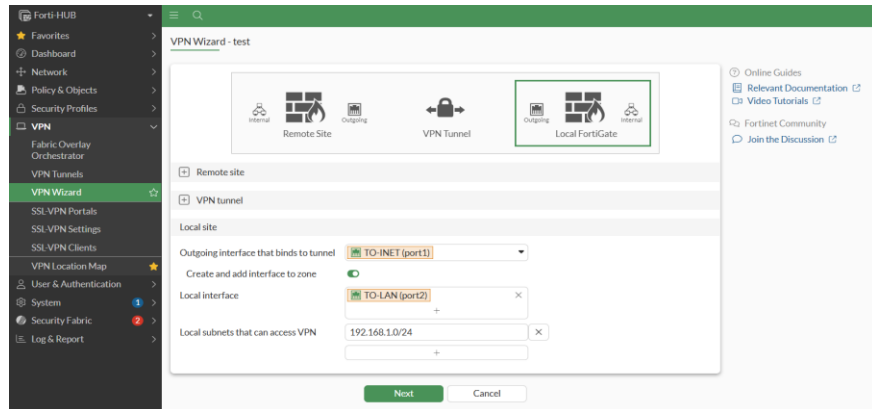
- Remote Device Type: Choose FortiGate.
- Click Next.
- Remote IP Address: Enter the public IP address of the Site B FortiGate.



- Outgoing Interface: Select your WAN interface.
- Pre-shared Key: Enter a strong, secret password. Write this down, as you will need to enter the exact same key on Site B.



- Click Next.
- Local Interface: Select your LAN interface.
- Local Subnets: The FortiGate will usually detect this automatically.
- Remote Subnets: Enter the LAN network subnet of Site B.



- Click Next.
- The wizard will show a summary of the objects and policies it will create automatically. Click Create.

2. Run the VPN Wizard on Site B:

- Repeat the exact same process on the Site B FortiGate, but with the values reversed:
 - Remote IP Address: Enter the public IP of Site A.
 - Pre-shared Key: Use the exact same key you created on Site A.
 - Remote Subnets: Enter the LAN subnet of Site A.

After both sides are configured, the IPsec tunnel will try to come up. You can monitor its status in Monitor > IPsec Monitor. If the status is Up (green), it means the two offices are now connected! Traffic between the local subnets will be automatically routed through the secure VPN tunnel.

Best Practices

- Strong Pre-shared Key: Use a long, random combination of uppercase and lowercase letters, numbers, and symbols for your IPsec key.
- Encryption Proposals: for maximum security, use strong encryption and hashing proposals (e.g., AES256 and SHA256) in your Phase 1 and Phase 2 IPsec VPN configurations.
- Dead Peer Detection: Enable this feature in the IPsec settings. It helps the FortiGate detect if the other side of the tunnel is down and tries to re-establish the connection faster.

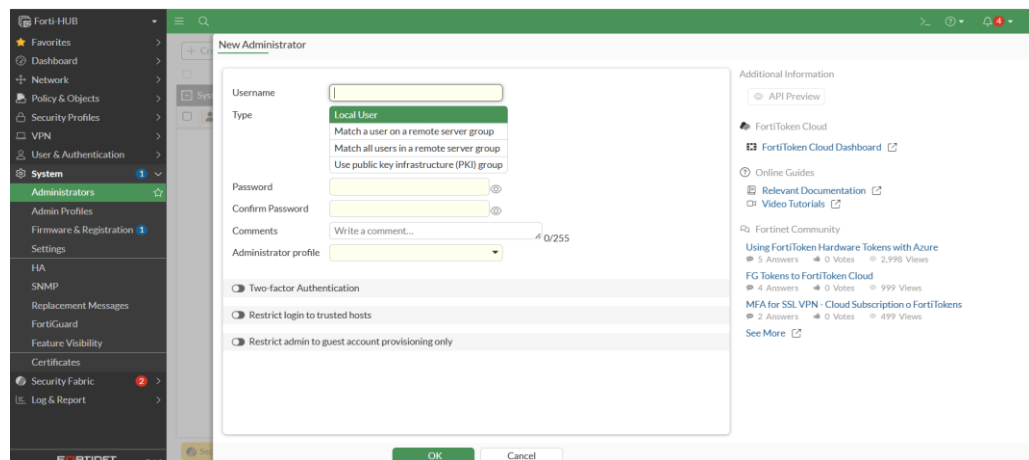
Chapter 7: Management, Logging, and Maintenance

Configuring a firewall is only half the job. Managing it, monitoring its activity, and maintaining it are key to long-term security.

7.1. Users and Authentication

You shouldn't just use the default admin account for everyone. Create administrator accounts with limited access rights.

- Navigate to System > Administrators. Click Create New > Administrator.



- Enter a username and password.
- For the Administrator Profile, don't always use super_admin. Create a custom profile in System > Admin Profiles. For example, you could create an audit_readonly profile that can only view configurations and logs, but cannot change anything. This is very useful for audit teams or junior staff.

7.2. Logging and Reporting

The FortiGate generates a huge amount of valuable log data. The key to understanding it is knowing where to look.

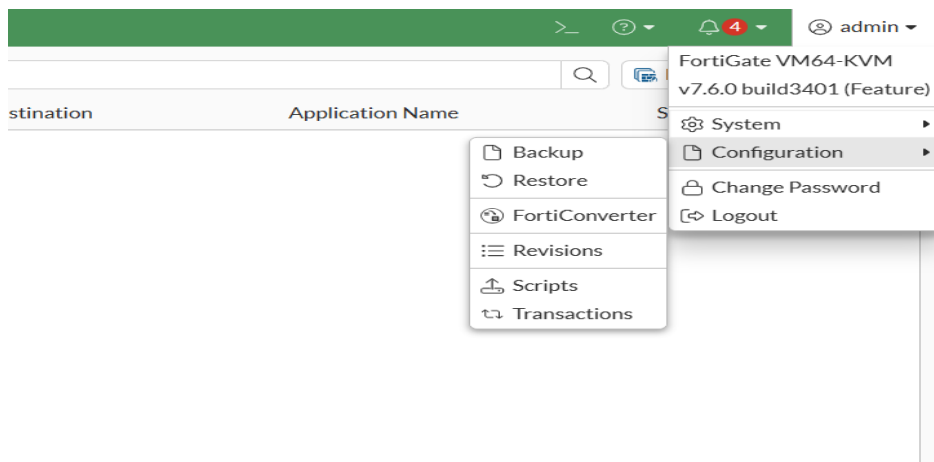
- Navigate to Log & Report.
- Forward Traffic: This is the log you'll look at most often. It shows all sessions that were allowed or denied by your firewall policies. It is essential for troubleshooting connectivity.
- Security Events: Here you will find logs from your Security Profiles (for example, Web Filter will show blocked sites, AntiVirus will show infected files).
- Local Reports: FortiGate can generate basic reports directly on the device. Navigate to Log & Report > Reports to view them.

For more serious logging and analysis, organizations typically use FortiAnalyzer (a separate appliance or VM) or the FortiCloud service to store and analyze logs over a long period.

7.3. Backing Up and Restoring Configurations

Do this regularly! Especially before making major changes or upgrading firmware.

- Navigate to the top right corner, click your admin name > Configuration > Backup.



- Save the .conf file in a safe location. You can also choose to encrypt the backup file with a password for added security.
- To restore, navigate to the same location, choose Restore, and upload your .conf file. The device will reboot with the restored configuration.

7.4. Basic Troubleshooting

When something isn't working, don't panic. The FortiGate has great built-in tools.

- **Policy Lookup:** Found in Policy & Objects > Firewall Policy. This tool lets you enter a source IP, destination, port, and protocol, and the FortiGate will tell you which policy the traffic would match. This is a great first step to diagnose access issues.
- **Packet Sniffer:** The FortiGate GUI has a built-in sniffer (Network > Packet Capture). You can choose an interface and apply filters (e.g., host or port) to see raw traffic in real-time.
- **CLI Diagnostics:** Open the CLI console. Some very useful commands are:
 - **diag debug flow:** This command is very detailed and will show you every step the FortiGate takes when processing a packet. Use it with filters so you are not overwhelmed by the output.
 - **execute ping <destination>:** To check basic connectivity.
 - **get system performance status:** To quickly see CPU and memory usage.

Best Practices

- **Schedule Backups:** Create a calendar reminder to back up the configuration on a weekly or monthly basis.
- **Centralized Logging:** If you manage more than one FortiGate, consider FortiAnalyzer or FortiCloud early on. It will greatly simplify your life.
- **Documentation:** Keep a record of significant configuration changes, explaining "why" the change was made.

Conclusion: The Next Steps in Your Fortinet Journey

Congratulations! You have completed the journey from firewall basics to configuring NGFW, VPNs, and essential management practices. You now have a strong foundation to manage and secure networks using FortiGate.

What You Have Learned:

- You understand the evolution from traditional firewalls to NGFW and the position of FortiGate in the security ecosystem.
- You are able to perform an initial configuration, including first-time access, registration, and firmware updates.
- You have mastered the core components of FortiGate: Objects and Firewall Policies.
- You can strengthen security with Security Profiles like Antivirus, Web Filter, and IPS.
- You understand and can configure NAT, for both outbound access (SNAT) and inbound access (DNAT/VIP).
- You are able to build secure tunnels using SSL-VPN for remote users and IPsec VPN for office-to-office connections.
- You know how to perform basic management, logging, and maintenance on the device.

Further Exploration: The world of Fortinet is vast. Here are some advanced topics you can explore:

- SD-WAN (Software-Defined WAN): Use FortiGate to intelligently route traffic over multiple internet connections (e.g., MPLS and broadband) to improve performance and reliability.
- Deeper Security Fabric: Integrate FortiGate with FortiSwitch, FortiAP, and FortiAnalyzer for comprehensive security visibility and automation.
- High Availability (HA): Configure two FortiGates in a cluster to ensure the network stays up and running even if one device fails.

Fortinet Certification: If you are serious about a career in network security with Fortinet products, consider getting certified. The most logical next step is the NSE 4 - Fortinet Network

Security Professional. The knowledge you've gained from this ebook is an excellent foundation for preparing for the NSE 4 exam.

Thank you for following this guide. Keep learning, experimenting in a lab environment, and building more secure networks.

<https://www.linkedin.com/in/gitesh-d-aa95a8227/>