Table of Contents

ACKNOWLEDGEMENT

I would like to express my heartfelt gratitude to all those who have contributed and supported me during the completion of this project titled "fortigate" at Texas College of Management and IT.

I am deeply indebted to my project guide [Manish Shakya] for their constant guidance, valuable insights, and unwavering support throughout this journey. Their expertise and encouragement have been instrumental in shaping the direction of this project.

I extend my sincere appreciation to the faculty members of the [IT department] for their valuable feedback and suggestions, which have been pivotal in improving the quality of this report.

My heartfelt thanks go to my friends for their encouragement, patience, and belief in my abilities, which provided me with the motivation to persevere and complete this project successfully.

Lastly, I want to acknowledge the boundless support from all the individuals and resources whose efforts have contributed to the accomplishment of this project.

Thank you all for being an essential part of this endeavor.

Group 1

BCS 3rd semStudent

Texas College of Management and IT

ABSTRACT

The project report titled "fortigate" presents a comprehensive exploration of a novel security solution designed to fortify information retrieval and management. In an era where data breaches and cyber threats have become increasingly prevalent, safeguarding sensitive information is of paramount importance. "fortigate" is an innovative system that aims to enhance data security while facilitating efficient data retrieval within organizations.

The project delves into the technical aspects of "Fortigate," elucidating its architecture, design principles, and implementation details. The system's intuitive user interface allows authorized personnel to retrieve data seamlessly while ensuring unauthorized access is thwarted. The report also sheds light on the performance evaluation of "Fortigate," demonstrating its efficiency and effectiveness in real-world scenarios.

INTRODUCTION TO FORTIGATE

The introduction provides a brief overview of the project "Fortigate - A Secure and Efficient Data Retrieval and Management System." It highlights the importance of data security and efficient data retrieval in the modern digital landscape. The introduction outlines the objectives of the project, which include enhancing data security, streamlining data retrieval, ensuring cross-platform compatibility, and allowing for scalability and future enhancements. It also introduces the methodology that will be followed to achieve the project's objectives, covering requirements analysis, literature review, system design, implementation, testing, and performance evaluation. The introduction concludes by emphasizing the significance of Fortigate in addressing data security challenges and empowering organizations to secure their valuable information effectively.

This project aims to provide a comprehensive understanding of FortiGate, a robust network security platform developed by Fortinet. FortiGate is a widely adopted security solution utilized by organizations to protect their networks from cyber threats, secure data, and ensure network performance and availability.

OBJECTIVES

Objective 1: Enhancing Data Security

The primary objective of the Fortigate project is to enhance data security within organizations. This involves the implementation of robust encryption algorithms to protect data at rest and during transit. By ensuring the confidentiality and integrity of sensitive information, Fortigate aims to prevent unauthorized access and potential data breaches.

Objective 2: Efficient Data Retrieval

The second objective is to facilitate efficient data retrieval for authorized personnel. Fortigate focuses on creating an intuitive user interface that allows seamless access to data while maintaining stringent access controls. By streamlining the retrieval process, Fortigate aims to improve productivity and user experience.

Objective 3: Implementing Multi-factor Authentication

To reinforce data security, the project aims to incorporate multi-factor authentication (MFA) mechanisms. MFA adds an extra layer of protection by requiring users to provide multiple forms of identification before accessing the system. By implementing MFA, Fortigate aims to thwart unauthorized access attempts and enhance overall system security.

Objective 4: Performance Evaluation

The project aims to evaluate the performance of the Fortigate in various real-world scenarios. This objective involves conducting rigorous testing and analysis to measure system efficiency, response times, and resource utilization. The results of the performance evaluation will be used to fine-tune and optimize the system.

Objective 5: Future Enhancements and Scalability

Finally, the report will address the objective of identifying potential areas for future enhancements and scalability. As technology and cybersecurity threats evolve, Fortigate must remain adaptable and capable of addressing new challenges. The project aims to explore avenues for expanding Fortigate's capabilities and integrating additional features in the future.

SCOPE OF FORTIGATE

The scope of Fortigate encompasses various aspects that define the boundaries and objectives of the project. It outlines the functionalities, target users, and potential applications of the Fortigate system. The following points highlight the scope of Fortigate:

1. Data Security Enhancement: Fortigate aims to significantly enhance data security within organizations by implementing robust encryption algorithms, access controls, and multi-factor authentication mechanisms. It focuses on safeguarding sensitive information from unauthorized access and potential data breaches.

2. Efficient Data Retrieval: The system targets the seamless and efficient retrieval of data for authorized personnel. Fortigate's user-friendly interface and streamlined data retrieval process aim to improve productivity and user experience.

3. Multi-factor Authentication Integration: Fortigate incorporates multi-factor authentication (MFA) to bolster data security. By requiring users to provide multiple forms of identification, the system ensures a higher level of authentication, reducing the risk of unauthorized access.

4. Intuitive User Interface: The scope of Fortigate includes the development of an intuitive and user-friendly interface. This allows users to interact with the system easily, even with minimal technical expertise.

5. Scalability and Future Enhancements: Fortigate is designed to be scalable, enabling it to accommodate the evolving needs of organizations and future advancements in technology. The scope includes provisions for future enhancements and expansions to adapt to changing cybersecurity requirements.

6. Cross-Platform Compatibility: Fortigate aims to be compatible with various platforms, including desktop computers, laptops, and mobile devices. This ensures accessibility from a range of devices and operating systems.

7. Real-World Performance Evaluation: The scope includes conducting a thorough performance evaluation of the Fortigate in real-world scenarios. The evaluation assesses its efficiency, response times, and resource utilization under different usage conditions.

IMPORTANCE OF THE PROJECT

The importance of Fortigate lies in its ability to address critical challenges related to data security and data retrieval in organizations. This innovative system offers several significant benefits:

Enhanced Data Security: Fortigate employs robust encryption algorithms and access controls to ensure the confidentiality and integrity of sensitive information. By safeguarding data at rest and during transmission, Fortigate helps organizations protect their valuable data assets from unauthorized access and potential cyber threats.

1. **Prevention of Data Breaches:** With its multi-factor authentication (MFA) mechanisms, Fortigate adds an extra layer of security, making it more difficult for unauthorized individuals to gain access to the system. This reduces the risk of data breaches, minimizing potential financial and reputational damages that organizations may face as a result of data leaks.

2. **Efficient Data Retrieval:** Fortigate streamlines the data retrieval process for authorized users. Its user-friendly interface and intuitive design enable seamless and quick access to relevant data, contributing to increased productivity and efficiency within the organization.

3. **Compliance and Regulations:** fortigate's adherence to data security regulations and compliance standards ensures that organizations can meet legal and industry requirements. This compliance is crucial, especially for organizations that handle sensitive data subject to various privacy and security regulations.

4. **Cross-Platform Compatibility:** Fortigate's compatibility with various platforms and devices enhances its accessibility and usability. Users can access the system from desktop computers, laptops, and mobile devices, ensuring that data retrieval and management can occur from different locations and devices.

5. **Scalability and Future-Proofing:** Fortigate's scalable design allows it to adapt to changing organizational needs and technological advancements. As an organization grows or faces new challenges, Fortigate can be expanded and updated to meet emerging security threats and requirements.

LIMITATIONS OF THE PROJECT

While Fortigate offers valuable benefits and features, it is essential to acknowledge its limitations to provide a comprehensive understanding of the project. The limitations of Fortigate include:

1. **Initial Implementation Challenges:** The initial implementation of Fortigate may pose challenges related to integration with existing data management systems and infrastructure within organizations. Ensuring smooth deployment and compatibility with diverse environments may require careful planning and coordination.

2. **Resource Requirements:** Fortigate's advanced security features, such as encryption and multi-factor authentication, may require additional computational resources, leading to higher hardware and processing costs for organizations with limited budgets.

3. **User Adoption and Training:** The adoption of new security measures and data retrieval processes may necessitate user training and adaptation to new workflows. Resistance or difficulty in adopting the system could impact its effectiveness until users become accustomed to the changes.

4. **Scalability Concerns:** As the organization grows and data volumes increase, fortigate's scalability may become a concern. Ensuring that the system can handle large-scale data retrieval and security requirements without compromising performance is essential.

5. **Dependency on Internet Connectivity:** Fortigate's cloud-based or network-dependent architecture may introduce a reliance on stable internet connectivity. Temporary connectivity issues or downtime could disrupt data retrieval and system accessibility.

6. **User Management Complexity:** Managing user access and authentication mechanisms, especially in large organizations, can become complex. Proper user management and access control require careful administration to prevent security gaps or access conflicts.

7. **Integration with Legacy Systems:** Integrating Fortigate with legacy systems or applications that lack modern security standards may present challenges. Ensuring secure communication and compatibility with older technologies can be time-consuming and may require additional development efforts

PROCEDURE

1. Physical Setup:

1. Connect the power adapter and turn on the device.
2. Connect a computer to one of FortiGate's Ethernet ports for initial configuration.

2. Network Configuration:

Configure the FortiGate's network interfaces based on your network topology and requirements. Set IP addresses, subnet masks, and gateway information.

Step 1: Accessing the FortiGate Web Interface

1. Connect a computer to the FortiGate using an Ethernet cable.
2. Open a web browser and enter the default IP address of the FortiGate (usually 192.168.1.99) in the address bar.
3. Log in with the administrator credentials. (username = admin & password = “blank”)

Step 2: Interface Configuration

1. Go to "Network" to "Interfaces."
2. Configure the interfaces based on your network topology:
3. Internal interfaces (LAN): Assign IP addresses and subnet masks to LAN interfaces connecting to internal networks.
4. External interfaces (WAN): Configure the WAN interface that connects to the internet or external network.
5. DMZ interfaces: If applicable, configure any demilitarized zone (DMZ) interfaces.

Step 3: IP Address Configuration

1. For the WAN interface, set the IP address provided by your ISP or configure it as per your network requirements. Choose between DHCP or static IP address based on your ISP's settings.
2. For LAN interfaces, assign IP addresses and subnet masks to match your internal network addressing scheme.

Step 4: Default Gateway Configuration

1. Configure the default gateway on the FortiGate to point to the next-hop gateway provided by your ISP for the WAN interface.
2. For LAN interfaces, the default gateway is usually FortiGate's own IP address on the corresponding interface.

Step 5: DNS Configuration

1. Set up DNS servers to resolve domain names. Go to "Network" to "DNS" and enter the IP addresses of your preferred DNS servers.

Step 6: Static Routes (if needed)

1. If you have multiple subnets or need to direct traffic to specific destinations, configure static routes. Go to "Network" to "Static Routes" and define the destination subnet and gateway.

Step 7: DHCP (if needed)

1. If you want the FortiGate to act as a DHCP server for your LAN, go to "Network" to "DHCP" and configure the DHCP server settings, including IP address range, lease time, and DNS servers to be provided to clients.

Step 8: Firewall Policies (optional)

1. If you need to allow or block traffic between different interfaces or subnets, set up firewall policies. Go to "Policy & Objects" to "IPv4 Policy" and create the necessary policies.

Step 9: Apply Configuration

1. Review your settings and click "Apply" to save the changes.

WAN Configuration:

Configure the WAN interface to connect to your internet service provider (ISP). Set the appropriate IP settings, such as DHCP or static IP if provided by your ISP.

Step 1: Accessing the FortiGate Web Interface

1. Connect a computer to the FortiGate using an Ethernet cable.
2. Open a web browser and enter the default IP address of the FortiGate (usually 192.168.1.99) in the address bar.
3. Log in with the administrator credentials.

Step 2: WAN Interface Configuration

1. Go to "Network" to "Interfaces."
2. Locate the WAN interface and click on it to configure its settings.
3. Choose the "Static" or "DHCP" option, depending on how your ISP provides the WAN IP address:

4. Static IP: If your ISP provides a static public IP address, select "Static" and enter the IP address, subnet mask, default gateway, and DNS server addresses provided by your ISP.
5. DHCP: If your ISP uses DHCP to dynamically assign the WAN IP address, select "DHCP" for the WAN interface. The FortiGate will automatically obtain the IP address, subnet mask, default gateway, and DNS servers from the ISP.

Step 3: PPPoE Configuration (if needed)

1. If your ISP requires PPPoE (Point-to-Point Protocol over Ethernet) authentication, select "PPPoE" for the WAN interface and enter the PPPoE username and password provided by your ISP.

Step 4: Additional WAN Settings (if needed)

Depending on your network setup and ISP requirements, you may need to configure additional settings like MTU (Maximum Transmission Unit), VLAN (Virtual LAN), or link speed/duplex mode for the WAN interface. Consult your ISP or network administrator for specific requirements.

Step 5: DNS Configuration

Set up DNS servers to resolve domain names. Go to "Network" to "DNS" and enter the IP addresses of your preferred DNS servers.

Step 6: Apply Configuration

Review your settings and click "Apply" to save the changes.

Firewall Policies:

Set up firewall policies to control traffic between different network segments and the internet. Define rules for allowing or blocking specific services and applications.

Step 1: Accessing the FortiGate Web Interface

Connect a computer to the FortiGate using an Ethernet cable.

Open a web browser and enter the default IP address of the FortiGate (usually 192.168.1.99) in the address bar.

Log in with the administrator credentials.

Step 2: Creating Firewall Policies

1. Go to "Policy & Objects" to "IPv4 Policy."
2. Click on "Create New" to add a new firewall policy.
3. Define the parameters for the firewall policy:
4. Source Interface: Select the interface where the traffic originates (e.g., LAN or WAN).
5. Source Address: Specify the source IP address or IP range for the traffic.
6. Destination Interface: Select the interface where the traffic is destined (e.g., LAN or WAN).
7. Destination Address: Specify the destination IP address or IP range for the traffic.
8. Schedule: Optionally, set a specific schedule for when the policy is active.
9. Service: Select the services or ports that the policy will allow or block.
10. Action: Choose "Accept" to allow the traffic or "Deny" to block it.
11. Logging: Enable logging to track traffic matching this policy.

VPN Setup:

Configure Virtual Private Networks (VPNs) if needed for secure remote access or site-to-site connectivity. Define authentication methods and encryption settings.

Step 1: Pre-configuration

1. Ensure that the FortiGate device has been set up with basic network configurations, including WAN and LAN interfaces.

Step 2: VPN Wizard

1. Log in to the FortiGate web-based management interface using a web browser.
2. Navigate to "VPN" to "IPsec Wizard."
3. Select "Site to Site" VPN and follow the wizard to configure the following parameters:
4. VPN Name: A descriptive name for the VPN.
5. Local Interface: Choose FortiGate's outgoing interface (usually the WAN interface).
6. Local Subnet: Define the local network subnet to be connected via the VPN.
7. Remote Gateway: Enter the IP address or domain name of the remote VPN gateway.
8. Remote Subnet: Define the remote network subnet to be connected via the VPN.
9. Authentication Method: Choose a pre-shared key or certificate-based authentication.
10. Pre-shared Key: If using pre-shared key authentication, enter the shared secret.
11. Phase 1 Proposal: Define the encryption and authentication algorithms for phase 1 of the VPN tunnel.
12. Phase 2 Proposal: Define the encryption and authentication algorithms for phase 2 of the VPN tunnel.
13. Key Life Time: Set the key lifetime for phase 1 and phase 2.

Step 3: Firewall Policies

- After creating the VPN tunnel, you may need to create firewall policies to allow traffic between the local and remote networks through the VPN tunnel. Go to "Policy & Objects" to "IPv4 Policy" and create the necessary policies.

Step 4: Testing : Test the VPN connectivity by sending traffic between the local and remote networks through the VPN tunnel.

Security Profiles:

Enable security profiles such as antivirus, intrusion prevention, and web filtering to protect against threats and malicious content.

1. Antivirus:

Scans incoming and outgoing traffic for known viruses and malware.

Blocks infected files from entering the network and prevents malware from spreading.

2. Intrusion Prevention System (IPS):

Inspects network traffic for known and unknown threats, including exploits and vulnerabilities.

Blocks malicious or suspicious activities in real-time.

3. Web Filtering:

Controls access to websites based on categories, URLs, or specific keywords.

Helps prevent users from accessing malicious or inappropriate content.

4. Application Control:

Manages and controls the usage of specific applications and services on the network.

Allows organizations to optimize bandwidth and enforce security policies.

5. Data Loss Prevention (DLP):

Monitors and controls data flow in and out of the network to prevent sensitive data leaks.

Enforces policies to comply with data protection regulations.

6. Advanced Threat Protection (ATP):

Includes sandboxing and behavior-based analysis to detect and mitigate zero-day threats.

Analyzes suspicious files and activities in a secure environment.

7. SSL Inspection:

Decrypts and inspects SSL/TLS encrypted traffic to detect hidden threats.

Helps protect against threats that might be hidden in encrypted communications.

8. Email Filtering (Anti-Spam):

Filters incoming emails to block spam, phishing attempts, and malicious attachments.

Helps maintain the security and integrity of email communications.

9. DNS Filtering:

Filters DNS queries to block access to malicious domains and prevent data exfiltration.

Web Filtering and Application Control:

Implement web filtering policies to restrict access to unwanted websites and create application control policies to manage application usage.

Regular Updates and Maintenance:

Keep the FortiGate firmware and security definitions up to date. Conduct periodic security assessments and update configurations based on changing requirements.

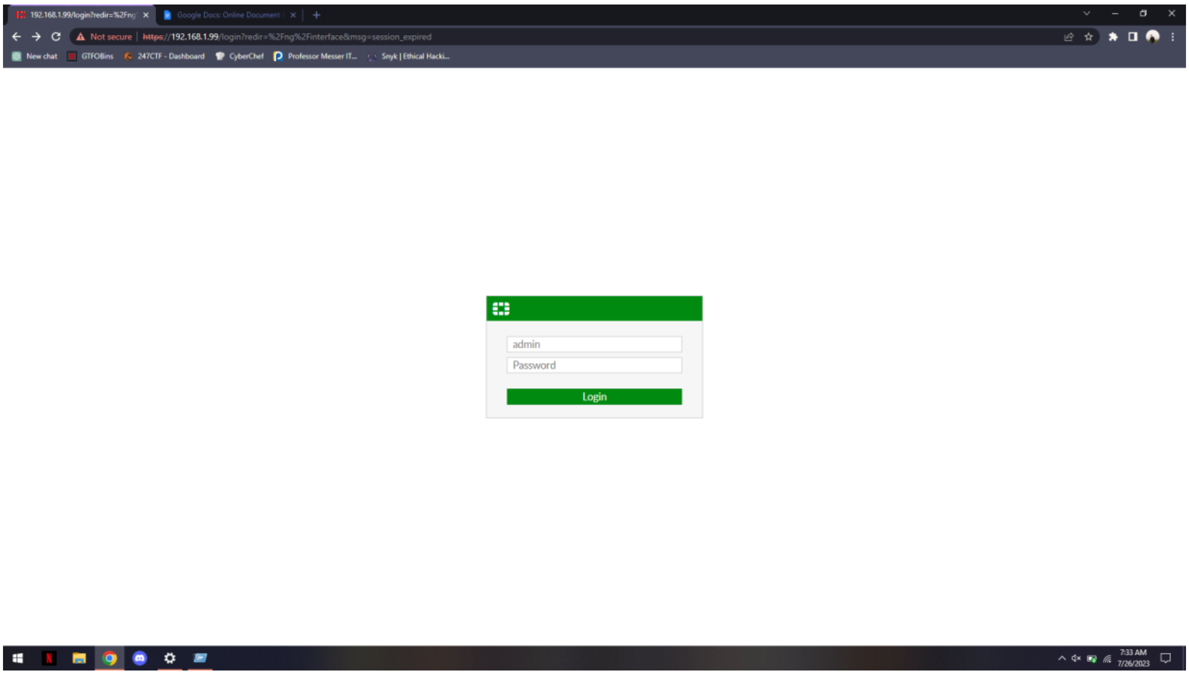
Continuous Monitoring:

Continuously monitor network traffic and security logs for potential threats or anomalies. Respond promptly to any security incidents.

CONCLUSION

The FortiGate project is a significant advancement in data security and efficiency. It addresses data protection challenges with encryption, access controls, and authentication. User-friendly interface enhances productivity. Consider initial challenges, resource needs, and user training. Regular maintenance and updates are crucial. FortiGate mitigates data breach risks, preserving reputation and trust. Continuous improvements ensure it remains effective in the evolving cybersecurity landscape. Overall, FortiGate is a reliable and valuable solution for secure data management

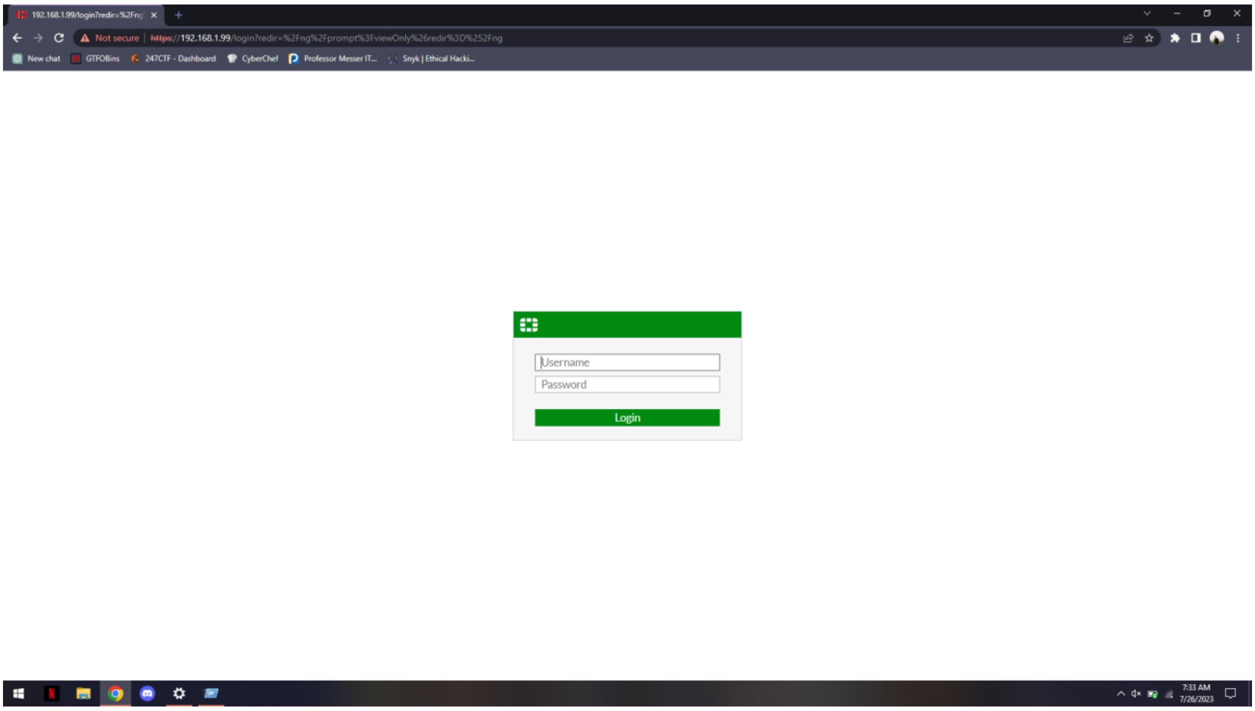
SCREENSHOTS



https://192.168.1.99/login?redir=%2Fng%2Finterface&msg=session_expired

admin

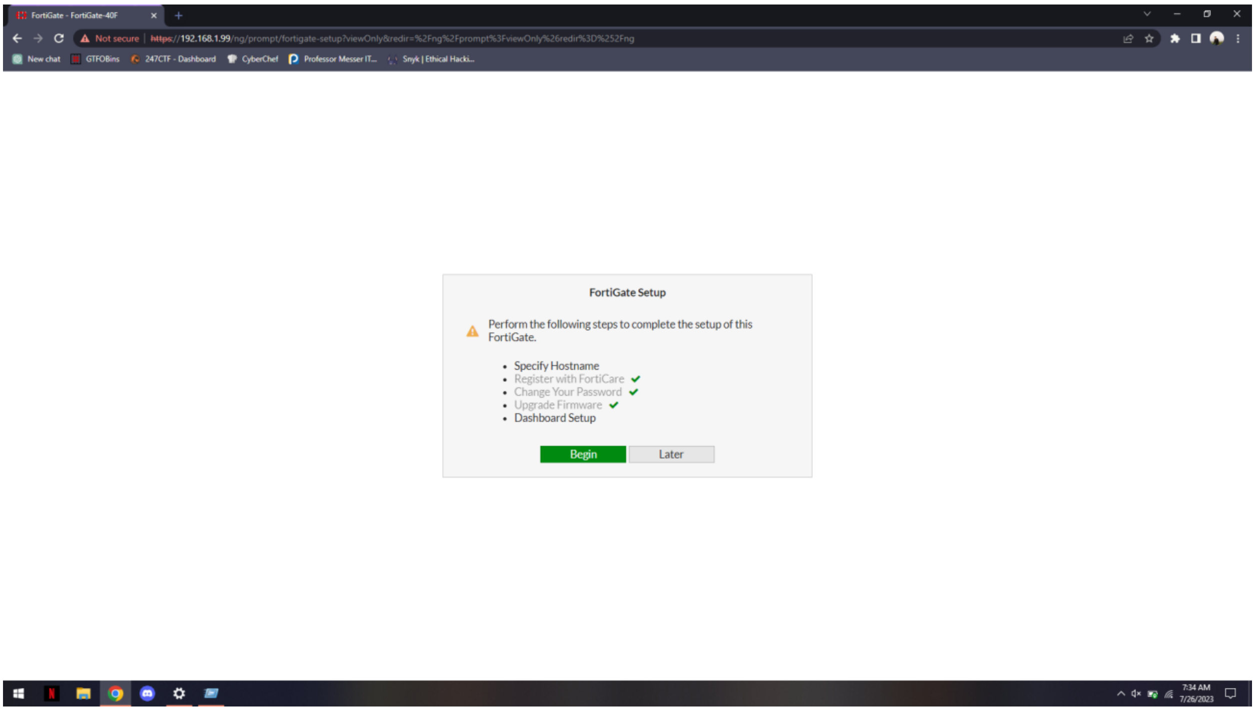
Password



https://192.168.1.99/login?redir=%2Fng%2Fprompt%3FviewOnly%26redir%3D%252Fng

Username

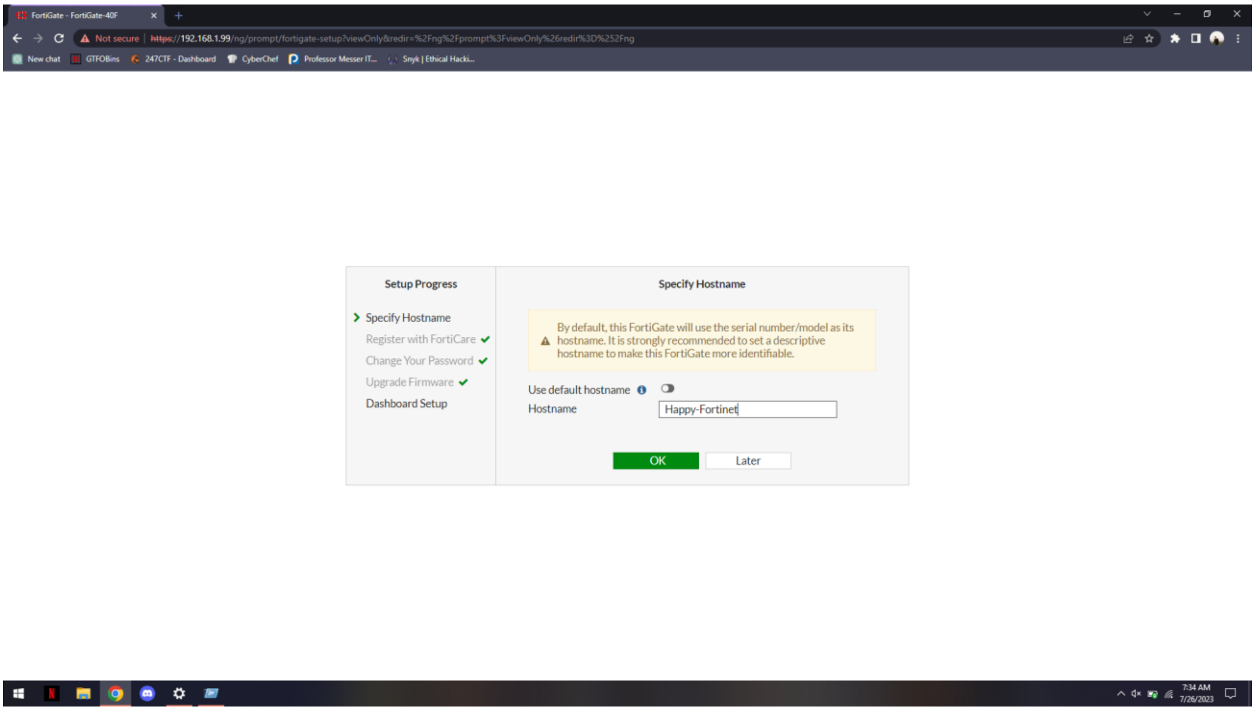
Password


FortiGate - FortiGate-40F
Not secure | https://192.168.1.99/ng/prompt/fortigate-setup?viewOnly&redir=%2Fng%2Fprompt%3FviewOnly%26redir%3D%252Fng
New chat GTFOBins 247CTF - Dashboard CyberChef Professor Messer IT... Snyk | Ethical Hacki...
7:34 AM
7/26/2023

FortiGate Setup

Perform the following steps to complete the setup of this FortiGate.

- Specify Hostname
- Register with FortiCare ✓
- Change Your Password ✓
- Upgrade Firmware ✓
- Dashboard Setup


FortiGate - FortiGate-40F
Not secure | https://192.168.1.99/ng/prompt/fortigate-setup?viewOnly&redir=%2Fng%2Fprompt%3FviewOnly%26redir%3D%252Fng
New chat GTFOBins 247CTF - Dashboard CyberChef Professor Messer IT... Snyk | Ethical Hacki...
7:34 AM
7/26/2023

Setup Progress

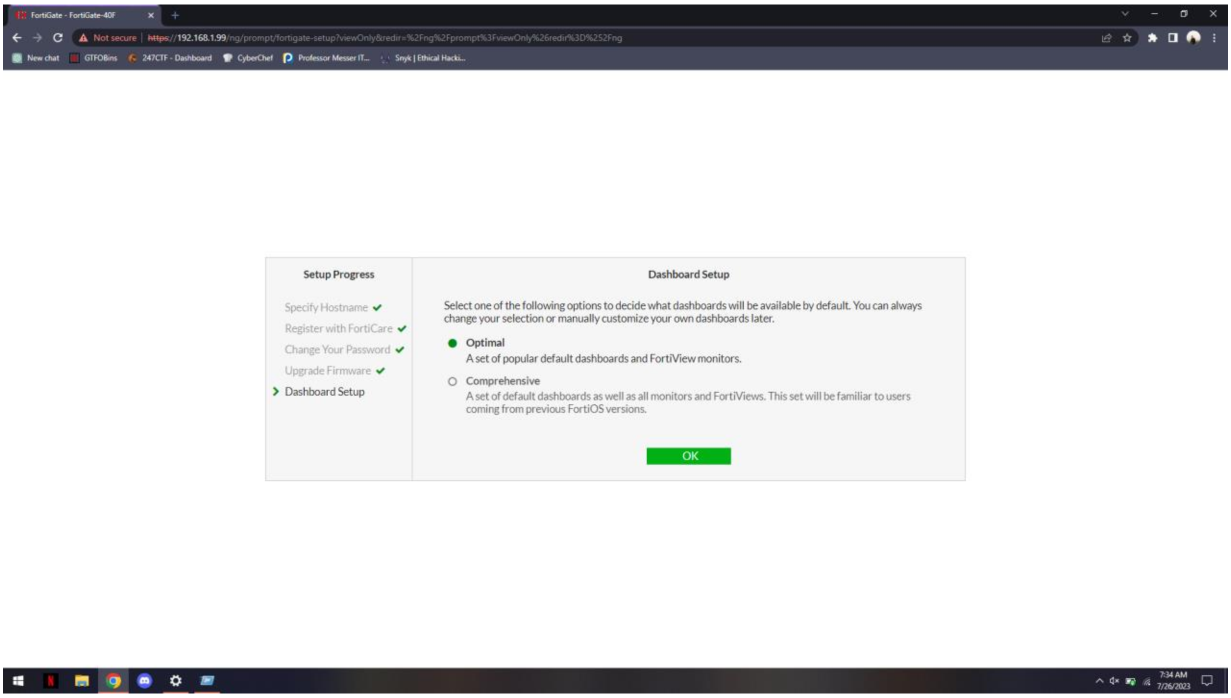
- Specify Hostname
- Register with FortiCare ✓
- Change Your Password ✓
- Upgrade Firmware ✓
- Dashboard Setup

Specify Hostname

By default, this FortiGate will use the serial number/model as its hostname. It is strongly recommended to set a descriptive hostname to make this FortiGate more identifiable.

Use default hostname ○

Hostname: Happy-Fortinet


FortiGate - FortiGate-40F
Not secure | https://192.168.1.99/ng/prompt/fortigate-setup?viewOnly&redir=%2Fng%2Fprompt%3FviewOnly%26redir%3D%252Fng
New chat
GTFOBins
247CTF - Dashboard
CyberChef
Professor Messer IT...
Snyk | Ethical Hacki...
7:34 AM
7/26/2023

Setup Progress

Specify Hostname ✓
Register with FortiCare ✓
Change Your Password ✓
Upgrade Firmware ✓
> Dashboard Setup

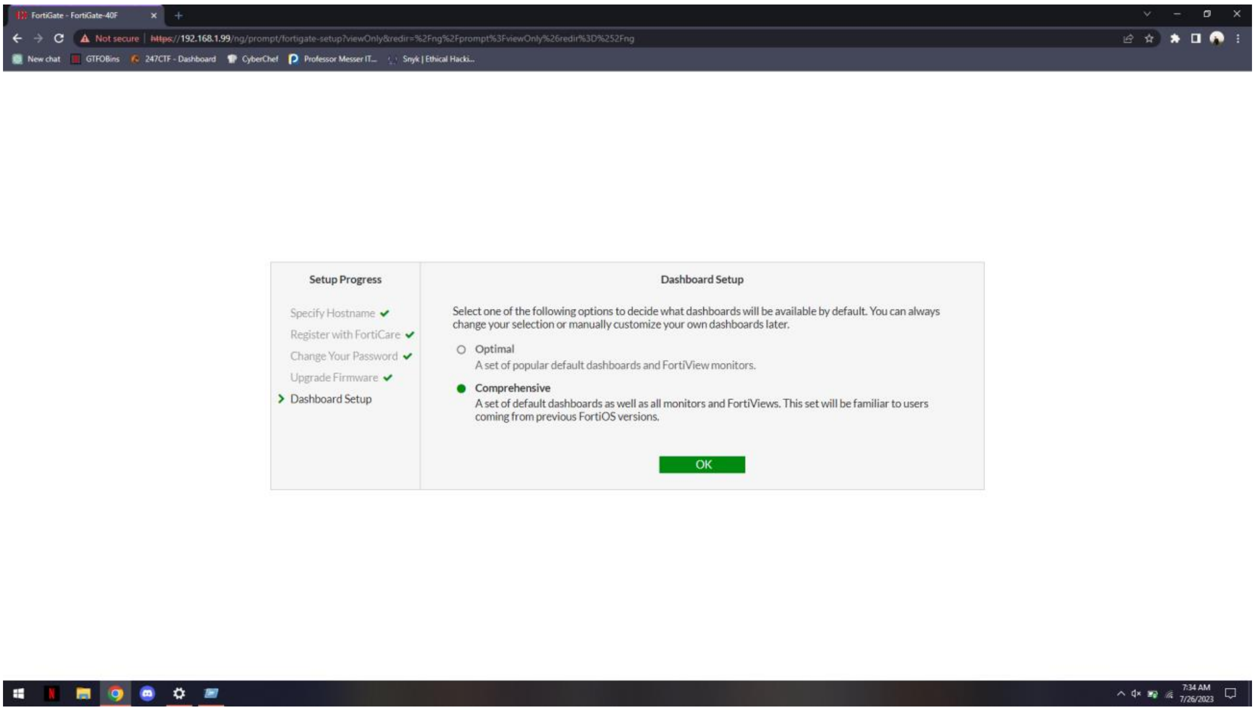
Dashboard Setup

Select one of the following options to decide what dashboards will be available by default. You can always change your selection or manually customize your own dashboards later.

● **Optimal**
A set of popular default dashboards and FortiView monitors.

○ Comprehensive
A set of default dashboards as well as all monitors and FortiViews. This set will be familiar to users coming from previous FortiOS versions.

OK


FortiGate - FortiGate-40F
Not secure | https://192.168.1.99/ng/prompt/fortigate-setup?viewOnly&redir=%2Fng%2Fprompt%3FviewOnly%26redir%3D%252Fng
New chat
GTFOBins
247CTF - Dashboard
CyberChef
Professor Messer IT...
Snyk | Ethical Hacki...
7:34 AM
7/26/2023

Setup Progress

Specify Hostname ✓
Register with FortiCare ✓
Change Your Password ✓
Upgrade Firmware ✓
> Dashboard Setup

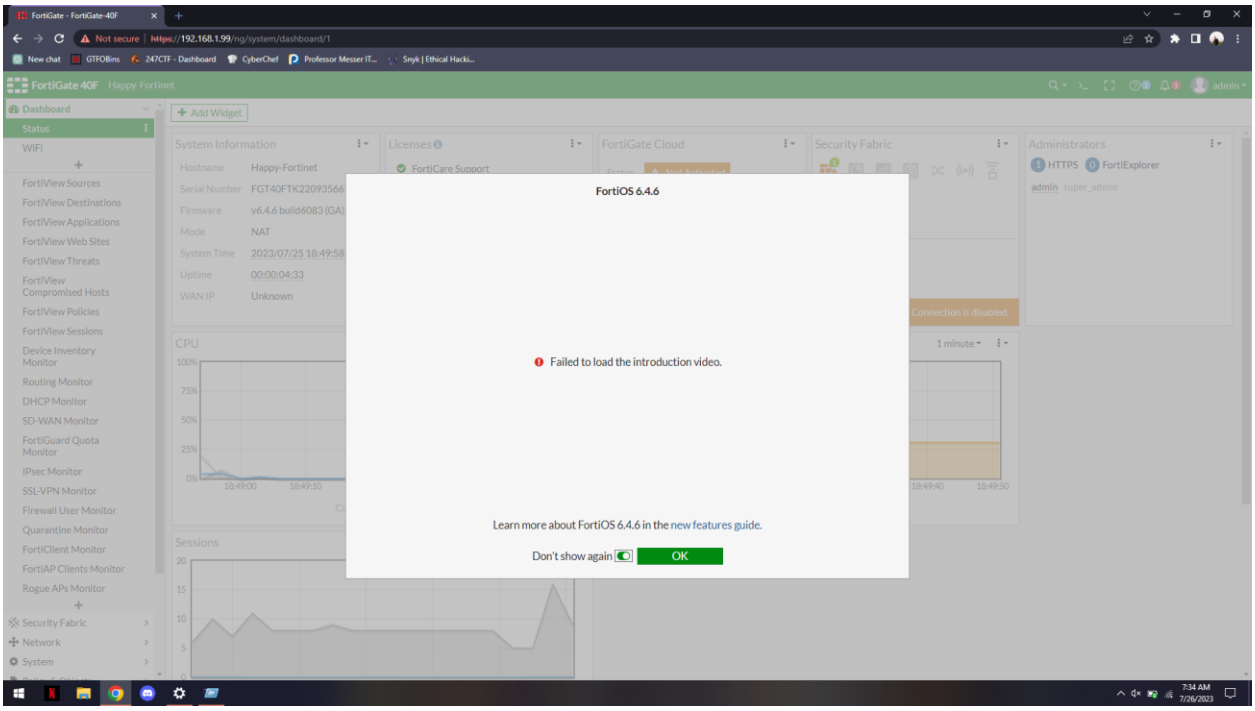
Dashboard Setup

Select one of the following options to decide what dashboards will be available by default. You can always change your selection or manually customize your own dashboards later.

○ Optimal
A set of popular default dashboards and FortiView monitors.

● **Comprehensive**
A set of default dashboards as well as all monitors and FortiViews. This set will be familiar to users coming from previous FortiOS versions.

OK



FortiOS 6.4.6

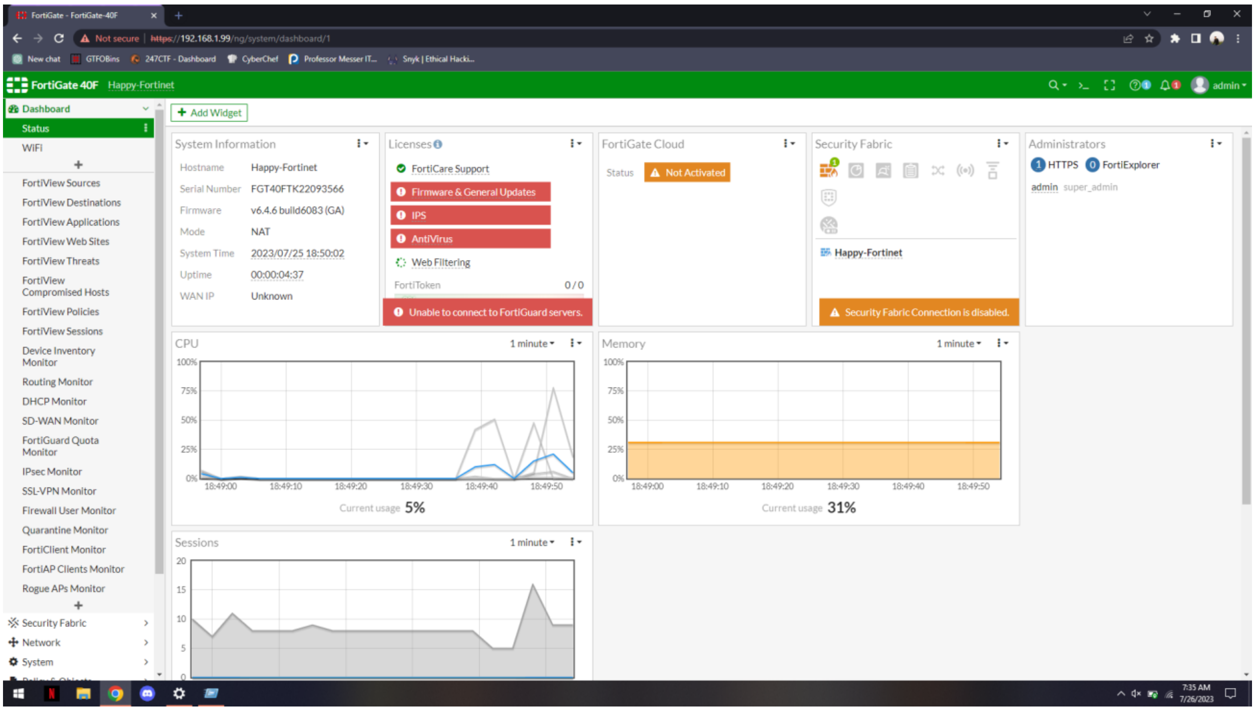
Failed to load the introduction video.

Learn more about FortiOS 6.4.6 in the new features guide.

Don't show again

OK

System Information
Hostname Happy-Fortinet
Serial Number FGT40FTK22093566
Firmware v6.4.6 build6083 (GA)
Mode NAT
System Time 2023/07/25 18:49:58
Uptime 00:00:04:33
WAN IP Unknown



System Information

Hostname	Happy-Fortinet
Serial Number	FGT40FTK22093566
Firmware	v6.4.6 build6083 (GA)
Mode	NAT
System Time	2023/07/25 18:50:02
Uptime	00:00:04:37
WAN IP	Unknown

Licenses

FortiCare Support

Firmware & General Updates

IPS

AntiVirus

Web Filtering

FortiToken 0 / 0

Unable to connect to FortiGuard servers.

FortiGate Cloud

Status Not Activated

Security Fabric

Happy-Fortinet

Security Fabric Connection is disabled.

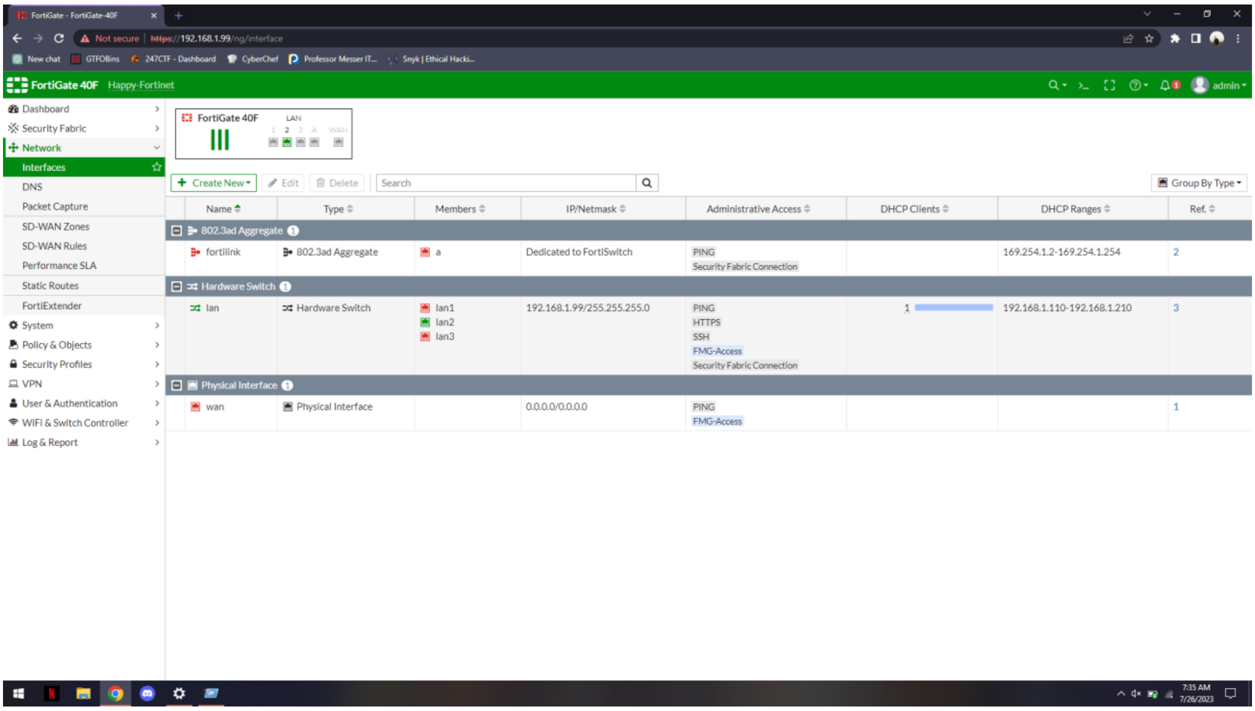
Administrators

1 HTTPS 0 FortiExplorer

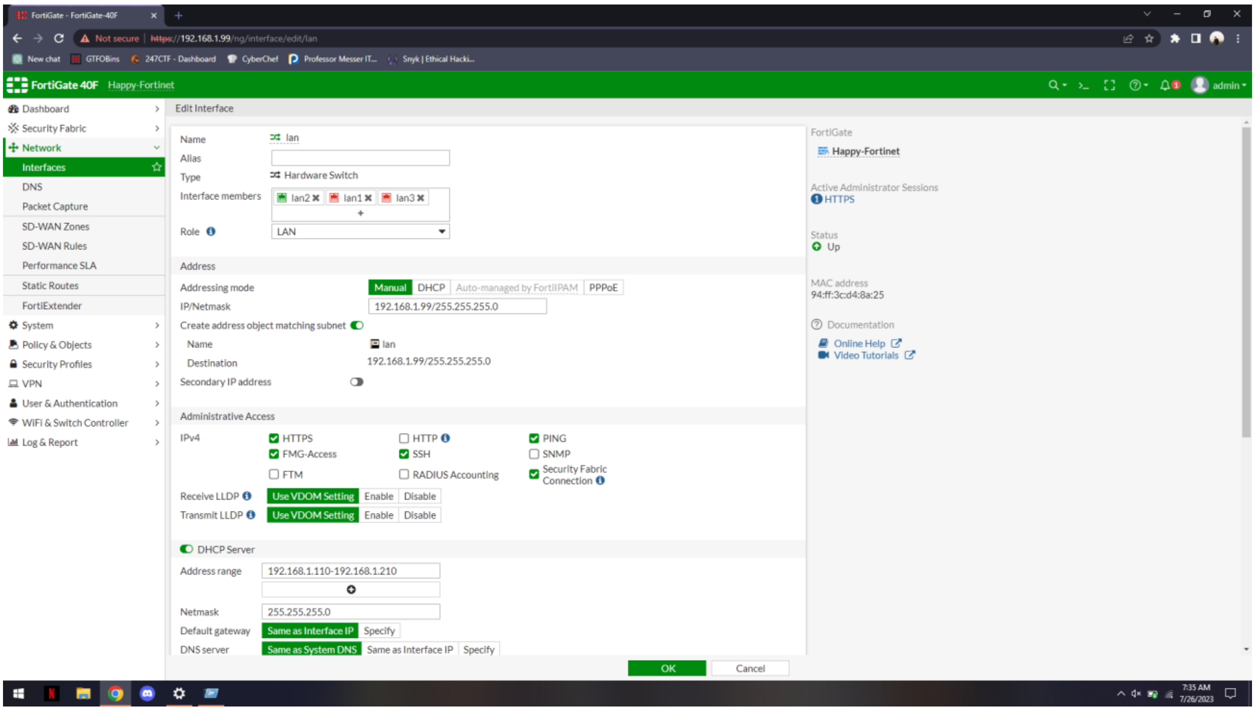
admin super_admin

CPU Current usage 5%

Memory Current usage 31%



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate	a	Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Hardware Switch 1							
lan	Hardware Switch	lan1 lan2 lan3	192.168.1.99/255.255.255.0	PING HTTPS SSH FMG-Access Security Fabric Connection	1	192.168.1.110-192.168.1.210	3
Physical Interface 1							
wan	Physical Interface		0.0.0.0/0.0.0.0	PING FMG-Access			1



Edit Interface

Name: lan

Alias:

Type: Hardware Switch

Interface members: lan2 ✖ lan1 ✖ lan3 ✖

Role: LAN

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by FortiIPAM PPPoE

IP/Netmask: 192.168.1.99/255.255.255.0

Create address object matching subnet ●

Name: lan

Destination: 192.168.1.99/255.255.255.0

Secondary IP address ○

Administrative Access

IPv4: ☑ HTTPS ☐ HTTP ☑ PING ☑ FMG-Access ☑ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting ☑ Security Fabric Connection

Receive LLDP: [✓ Use VDOM Setting] Enable Disable

Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

● DHCP Server

Address range: 192.168.1.110-192.168.1.210

Netmask: 255.255.255.0

Default gateway: [✓ Same as Interface IP] Specify

DNS server: [✓ Same as System DNS] Same as Interface IP Specify

FortiGate: Happy-Fortinet

Active Administrator Sessions: 1 HTTPS

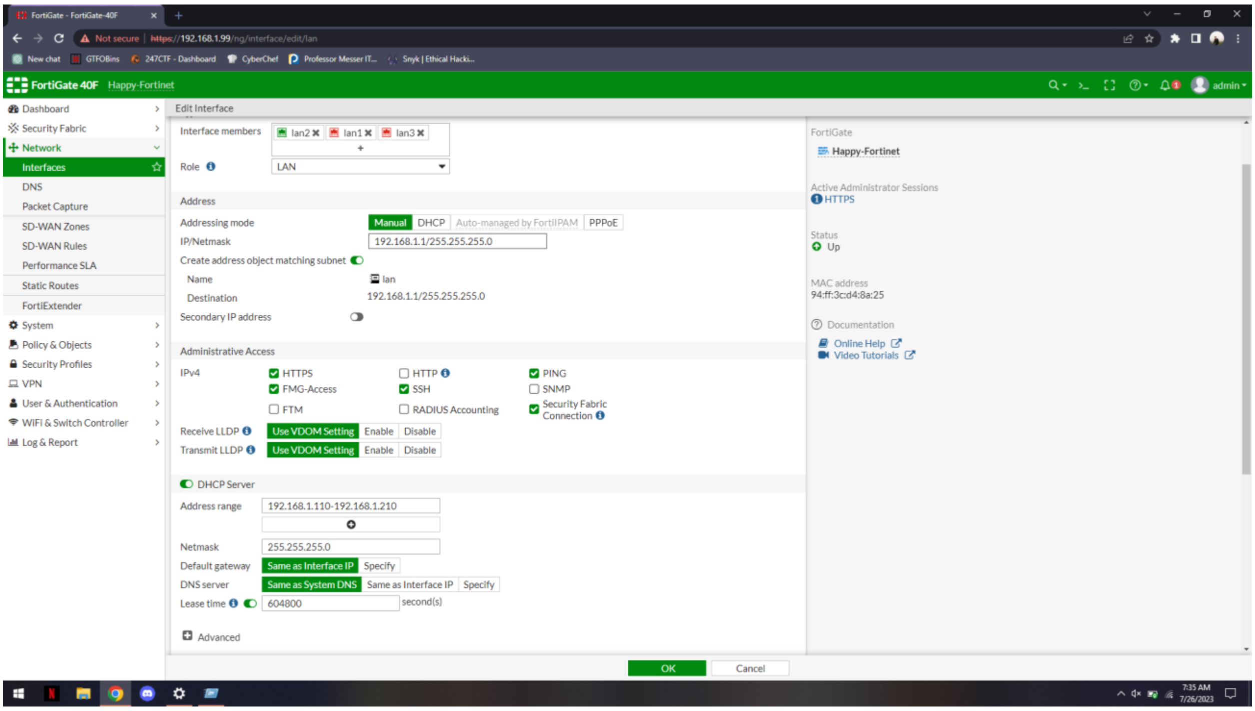
Status: Up

MAC address: 94:ff:3c:d4:8a:25

Documentation

Online Help

Video Tutorials



Edit Interface

Interface members: lan2 ✖ lan1 ✖ lan3 ✖

Role: LAN

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by FortiIPAM PPPoE

IP/Netmask: 192.168.1.1/255.255.255.0

Create address object matching subnet: ●

Name: lan

Destination: 192.168.1.1/255.255.255.0

Secondary IP address: ○

Administrative Access

IPv4: ☑ HTTPS □ HTTP ☑ PING ☑ FMG-Access ☑ SSH □ SNMP □ FTM □ RADIUS Accounting ☑ Security Fabric Connection

Receive LLDP: [✓ Use VDOM Setting] Enable Disable

Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

● DHCP Server

Address range: 192.168.1.110-192.168.1.210

Netmask: 255.255.255.0

Default gateway: [✓ Same as Interface IP] Specify

DNS server: [✓ Same as System DNS] Same as Interface IP Specify

Lease time: ● 604800 second(s)

Advanced

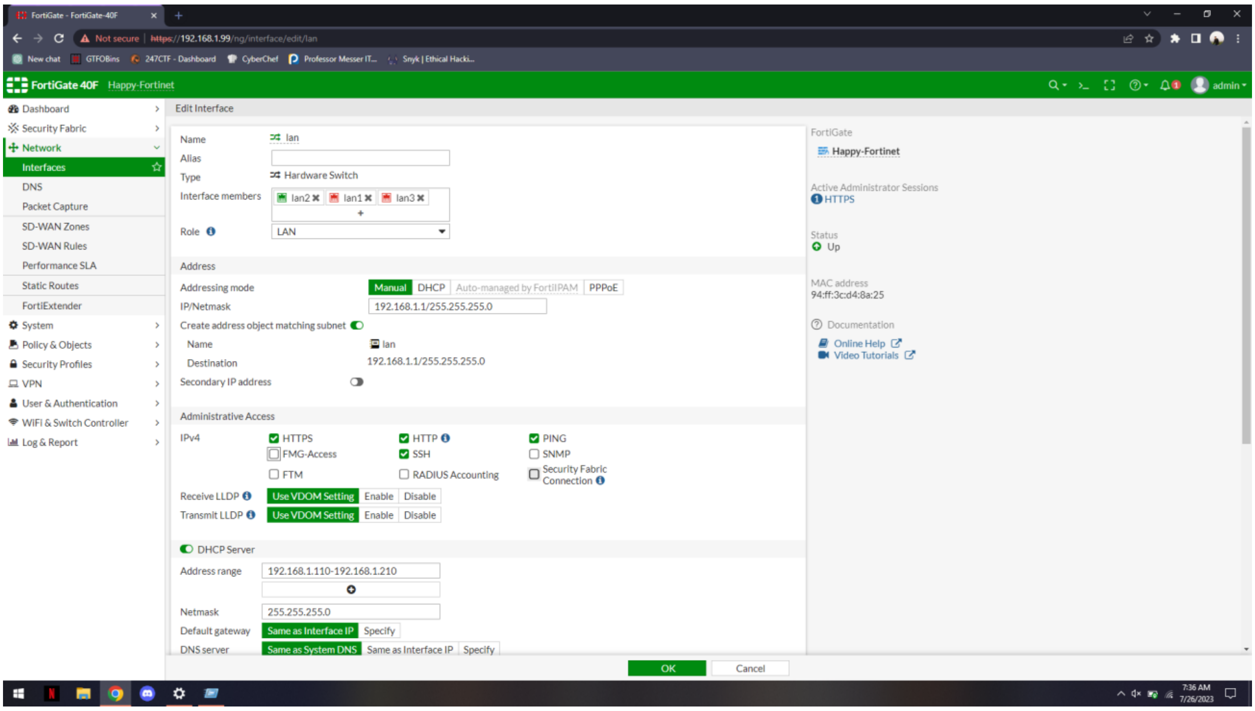
FortiGate: Happy-Fortinet

Active Administrator Sessions: 1 HTTPS

Status: Up

MAC address: 94:ff:3c:d4:8a:25

Documentation: Online Help, Video Tutorials



Edit Interface

Name: lan

Alias:

Type: Hardware Switch

Interface members: lan2 ✖ lan1 ✖ lan3 ✖

Role: LAN

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by FortiIPAM PPPoE

IP/Netmask: 192.168.1.1/255.255.255.0

Create address object matching subnet: ●

Name: lan

Destination: 192.168.1.1/255.255.255.0

Secondary IP address: ○

Administrative Access

IPv4: ☑ HTTPS ☑ HTTP ☑ PING □ FMG-Access ☑ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection

Receive LLDP: [✓ Use VDOM Setting] Enable Disable

Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

● DHCP Server

Address range: 192.168.1.110-192.168.1.210

Netmask: 255.255.255.0

Default gateway: [✓ Same as Interface IP] Specify

DNS server: [✓ Same as System DNS] Same as Interface IP Specify

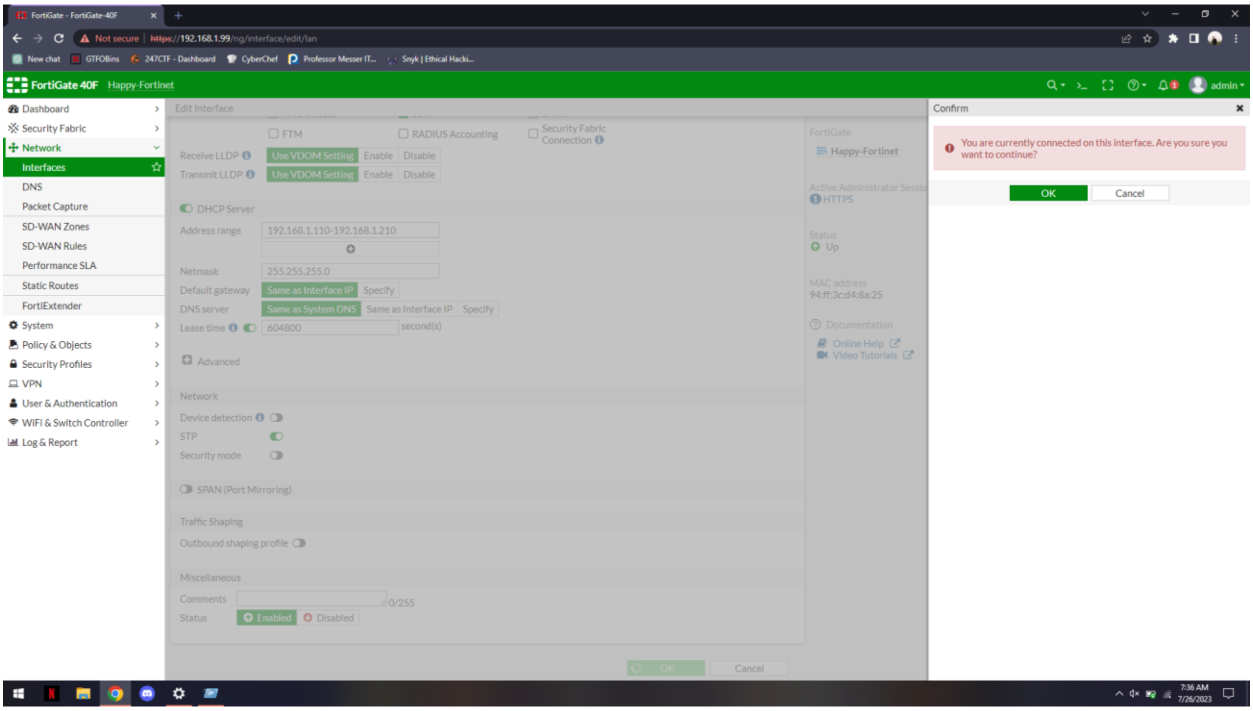
FortiGate: Happy-Fortinet

Active Administrator Sessions: 1 HTTPS

Status: Up

MAC address: 94:ff:3c:d4:8a:25

Documentation: Online Help, Video Tutorials



Confirm

You are currently connected on this interface. Are you sure you want to continue?

Edit Interface

□ FTM □ RADIUS Accounting □ Security Fabric Connection

Receive LLDP: Use VDOM Setting | Enable | Disable

Transmit LLDP: Use VDOM Setting | Enable | Disable

DHCP Server

Address range: 192.168.1.110-192.168.1.210

Netmask: 255.255.255.0

Default gateway: Same as Interface IP | Specify

DNS server: Same as System DNS | Same as Interface IP | Specify

Lease time: 604800 second(s)

Advanced

Network

Device detection

STP

Security mode

SPAN (Port Mirroring)

Traffic Shaping

Outbound shaping profile

Miscellaneous

Comments 0/255

Status: Enabled | Disabled

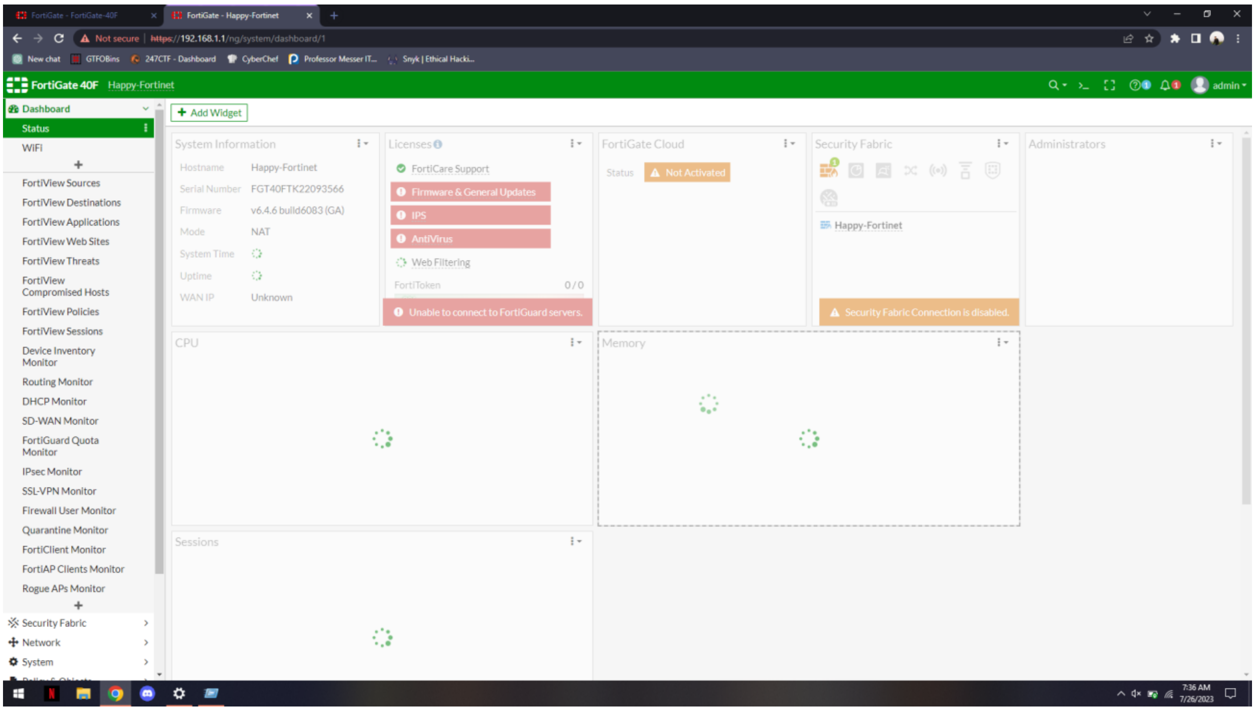
FortiGate: Happy-Fortinet

Active Administrator Sessions: HTTPS

Status: Up

MAC address: 94:ff:3c:d4:8a:25

Documentation: Online Help, Video Tutorials



System Information

Hostname	Happy-Fortinet
Serial Number	FGT40FTK22093566
Firmware	v6.4.6 build6083 (GA)
Mode	NAT
System Time	
Uptime	
WAN IP	Unknown

Licenses

- FortiCare Support
- Firmware & General Updates
- IPS
- AntiVirus
- Web Filtering
- FortiToken 0 / 0

Unable to connect to FortiGuard servers.

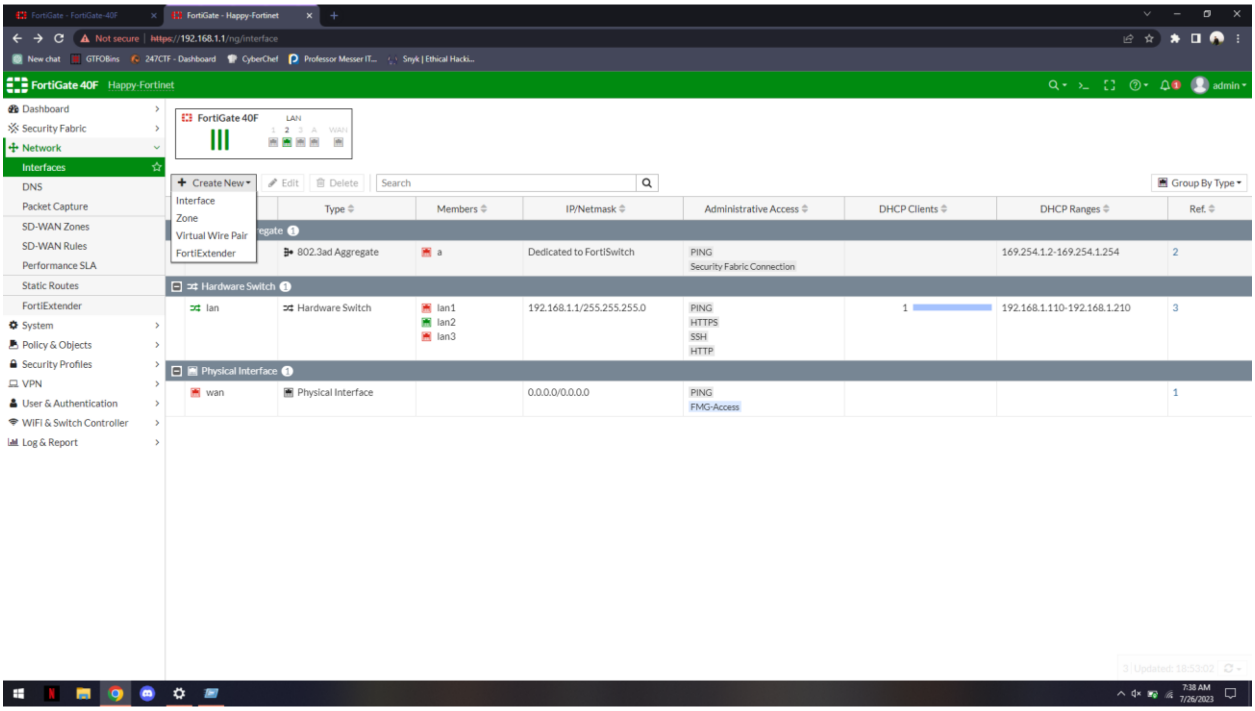
FortiGate Cloud

Status: Not Activated

Security Fabric

Happy-Fortinet

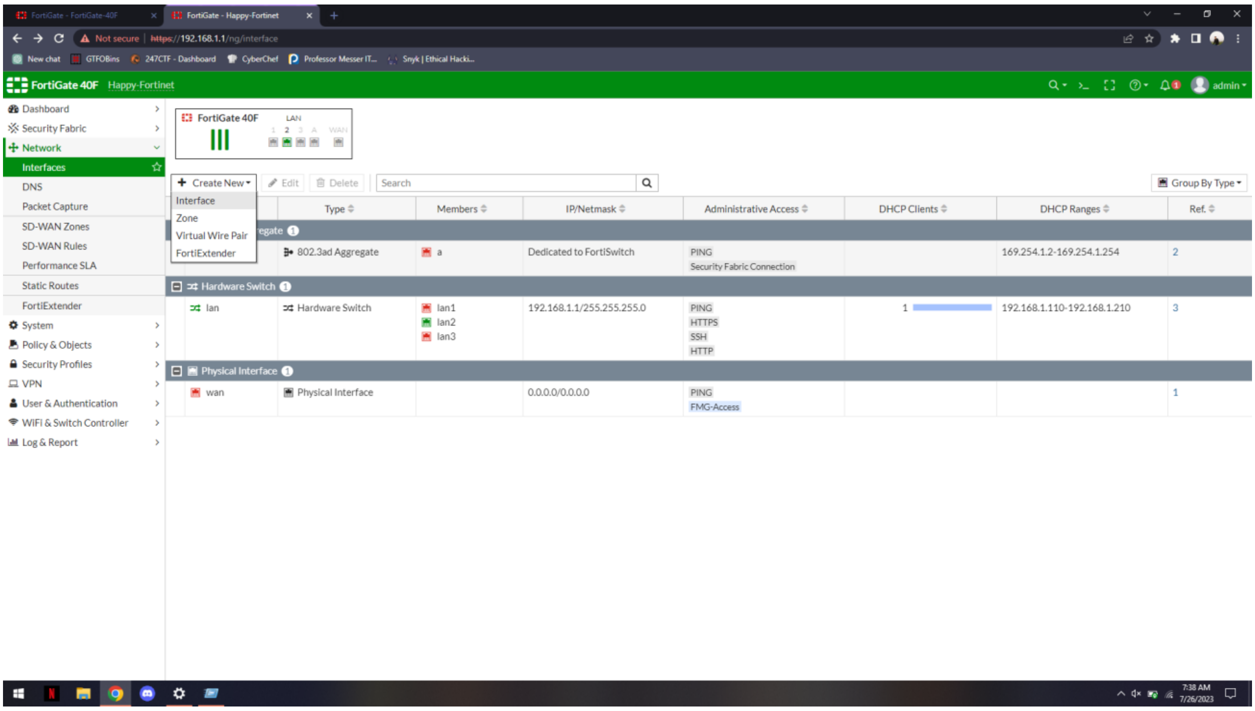
Security Fabric Connection is disabled.



FortiGate 40F Happy-Fortinet

Create New ▾ | Interface | Zone | Virtual Wire Pair | FortiExtender

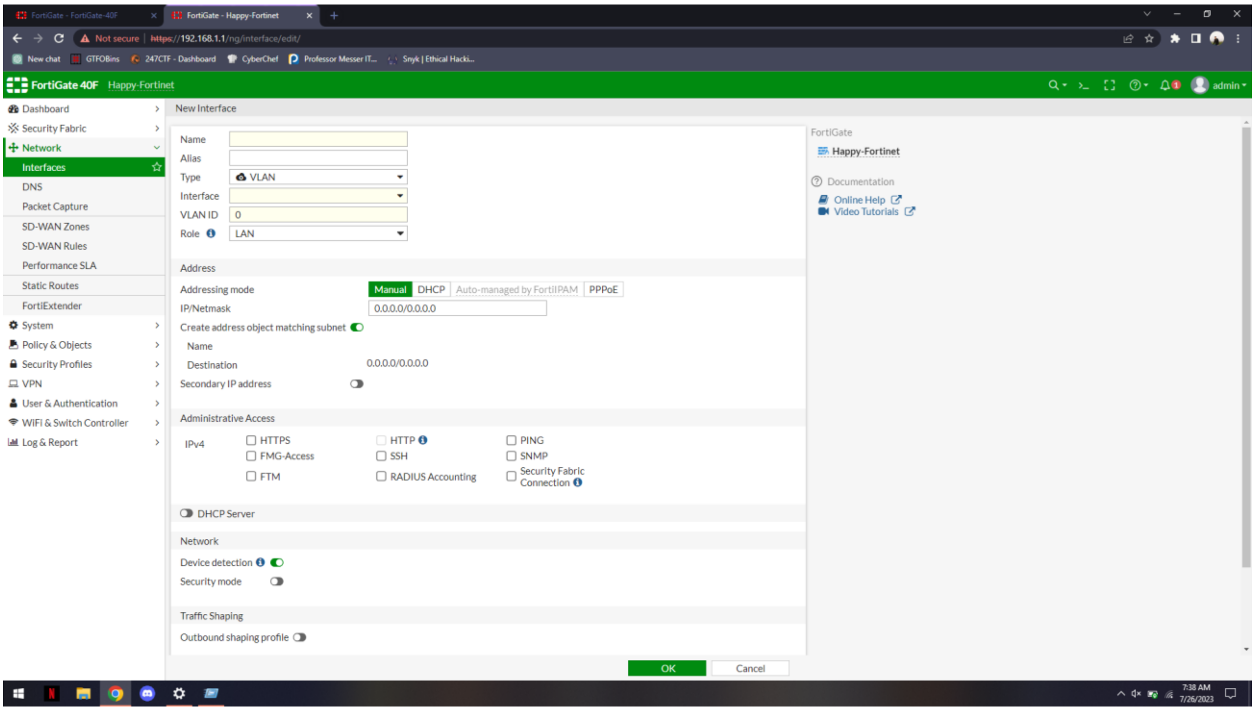
	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
…egate 1							
	802.3ad Aggregate	a	Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Hardware Switch 1							
lan	Hardware Switch	lan1 lan2 lan3	192.168.1.1/255.255.255.0	PING HTTPS SSH HTTP	1	192.168.1.110-192.168.1.210	3
Physical Interface 1							
wan	Physical Interface		0.0.0.0/0.0.0.0	PING FMG-Access			1



FortiGate 40F Happy-Fortinet

Create New ▾ | Interface | Zone | Virtual Wire Pair | FortiExtender

	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
…egate 1							
	802.3ad Aggregate	a	Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Hardware Switch 1							
lan	Hardware Switch	lan1 lan2 lan3	192.168.1.1/255.255.255.0	PING HTTPS SSH HTTP	1	192.168.1.110-192.168.1.210	3
Physical Interface 1							
wan	Physical Interface		0.0.0.0/0.0.0.0	PING FMG-Access			1



New Interface

Name:
Alias:
Type: VLAN
Interface:
VLAN ID: 0
Role: LAN

Address
Addressing mode: Manual | DHCP | Auto-managed by FortiIPAM | PPPoE
IP/Netmask: 0.0.0.0/0.0.0.0
Create address object matching subnet: ●
Name
Destination: 0.0.0.0/0.0.0.0
Secondary IP address: ○

Administrative Access
IPv4: □ HTTPS □ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection

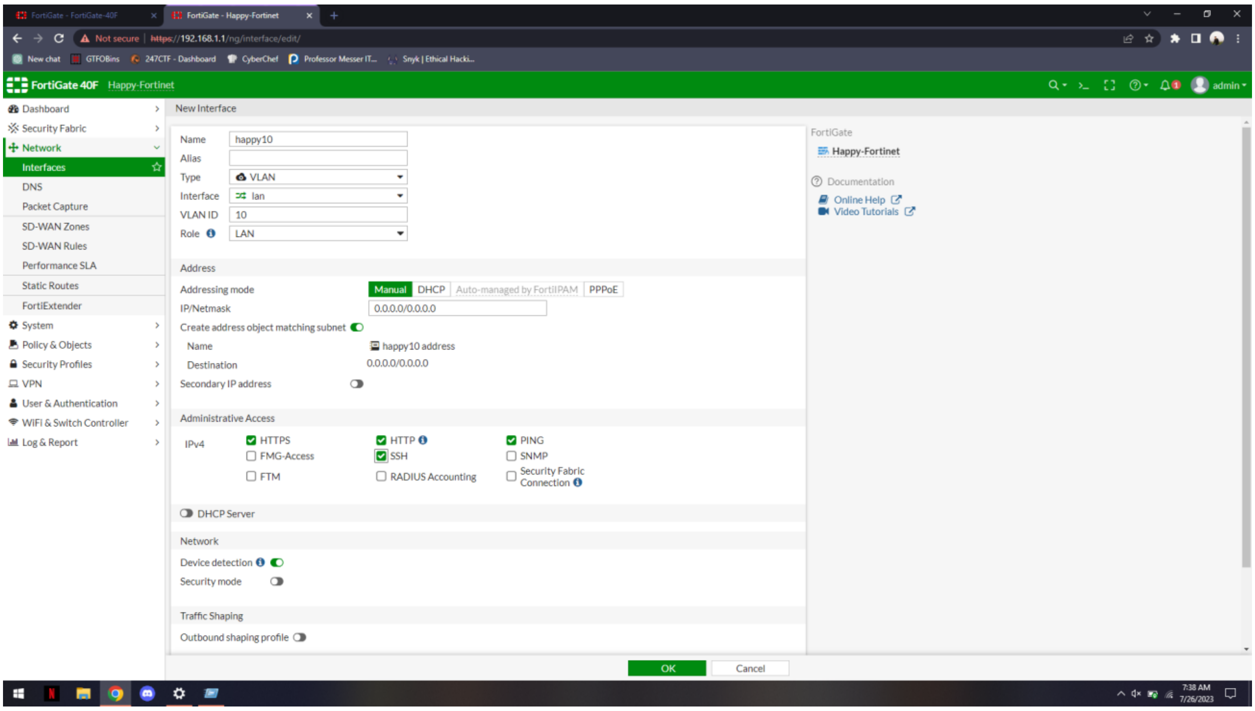
○ DHCP Server

Network
Device detection: ●
Security mode: ○

Traffic Shaping
Outbound shaping profile: ○

OK Cancel

-



New Interface

Name: happy10
Alias:
Type: VLAN
Interface: lan
VLAN ID: 10
Role: LAN

Address
Addressing mode: Manual | DHCP | Auto-managed by FortiIPAM | PPPoE
IP/Netmask: 0.0.0.0/0.0.0.0
Create address object matching subnet: ●
Name: happy10 address
Destination: 0.0.0.0/0.0.0.0
Secondary IP address: ○

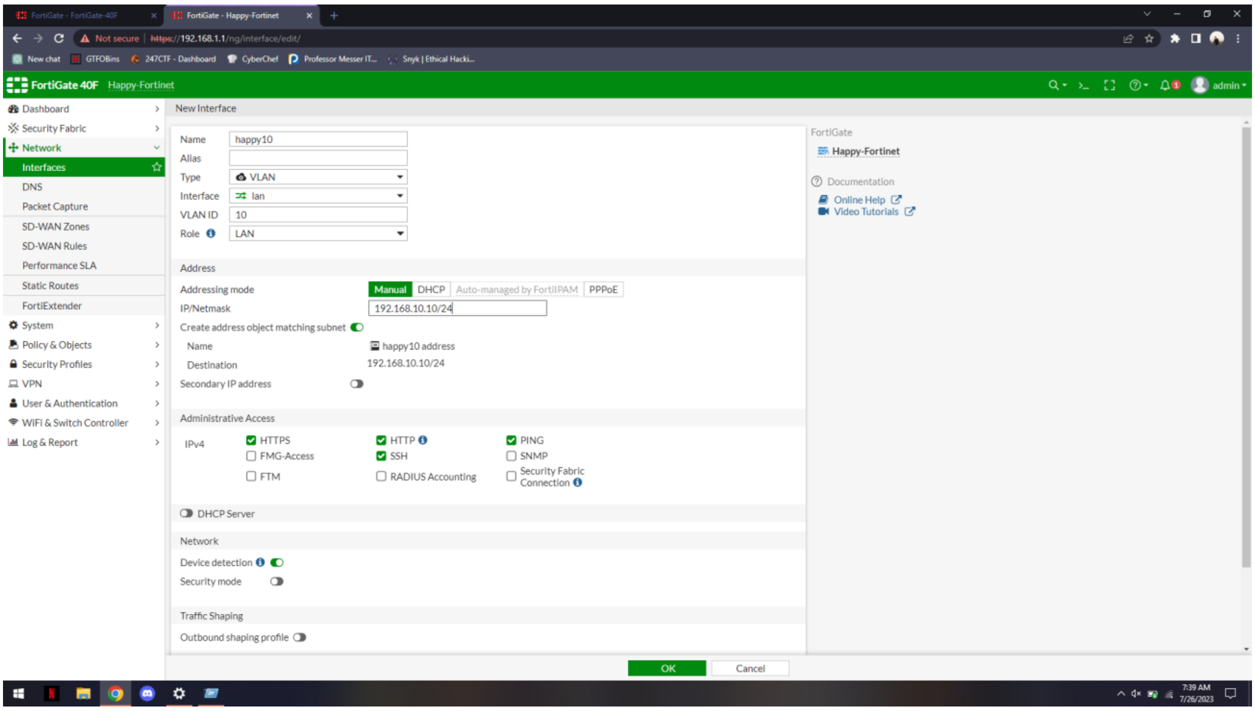
Administrative Access
IPv4: ☑ HTTPS ☑ HTTP ☑ PING □ FMG-Access ☑ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection

○ DHCP Server

Network
Device detection: ●
Security mode: ○

Traffic Shaping
Outbound shaping profile: ○

OK Cancel



New Interface

Name: happy10
Alias:
Type: VLAN
Interface: lan
VLAN ID: 10
Role: LAN

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by FortiIPAM PPPoE
IP/Netmask: 192.168.10.10/24
Create address object matching subnet: ●
Name: happy10 address
Destination: 192.168.10.10/24
Secondary IP address: ○

Administrative Access

IPv4
☑ HTTPS ☑ HTTP ☑ PING
☐ FMG-Access ☑ SSH ☐ SNMP
☐ FTM ☐ RADIUS Accounting ☐ Security Fabric Connection

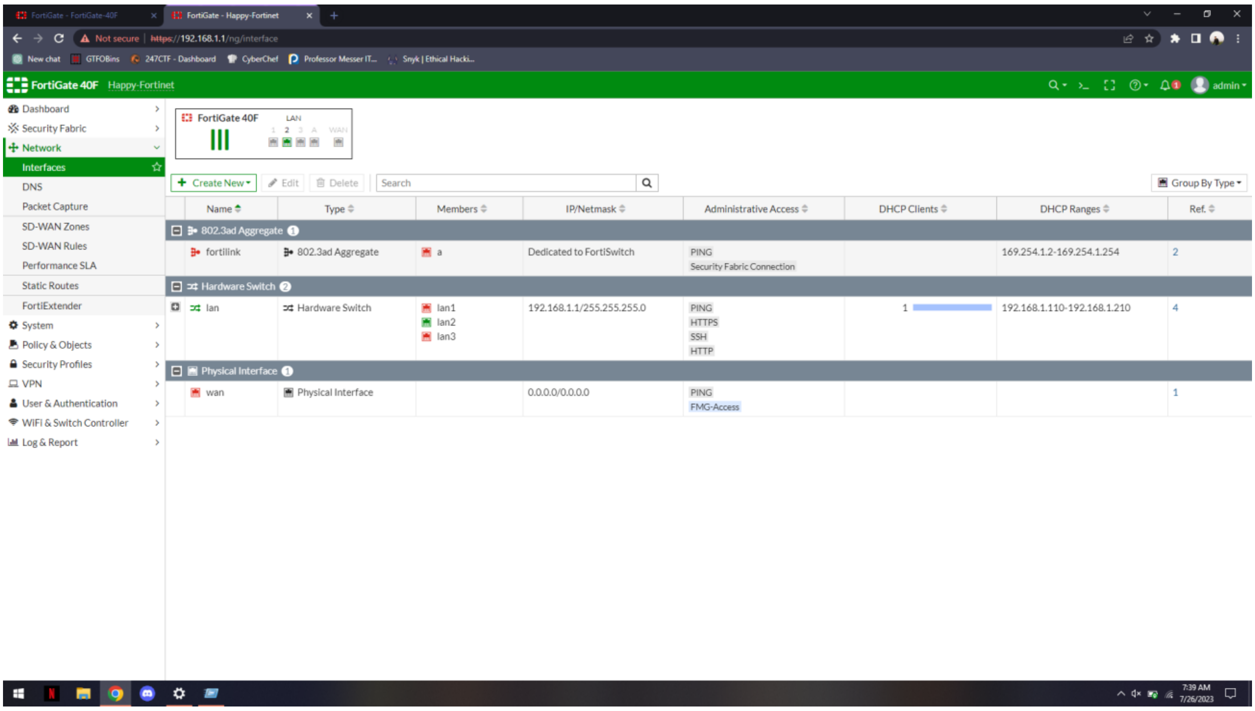
○ DHCP Server

Network

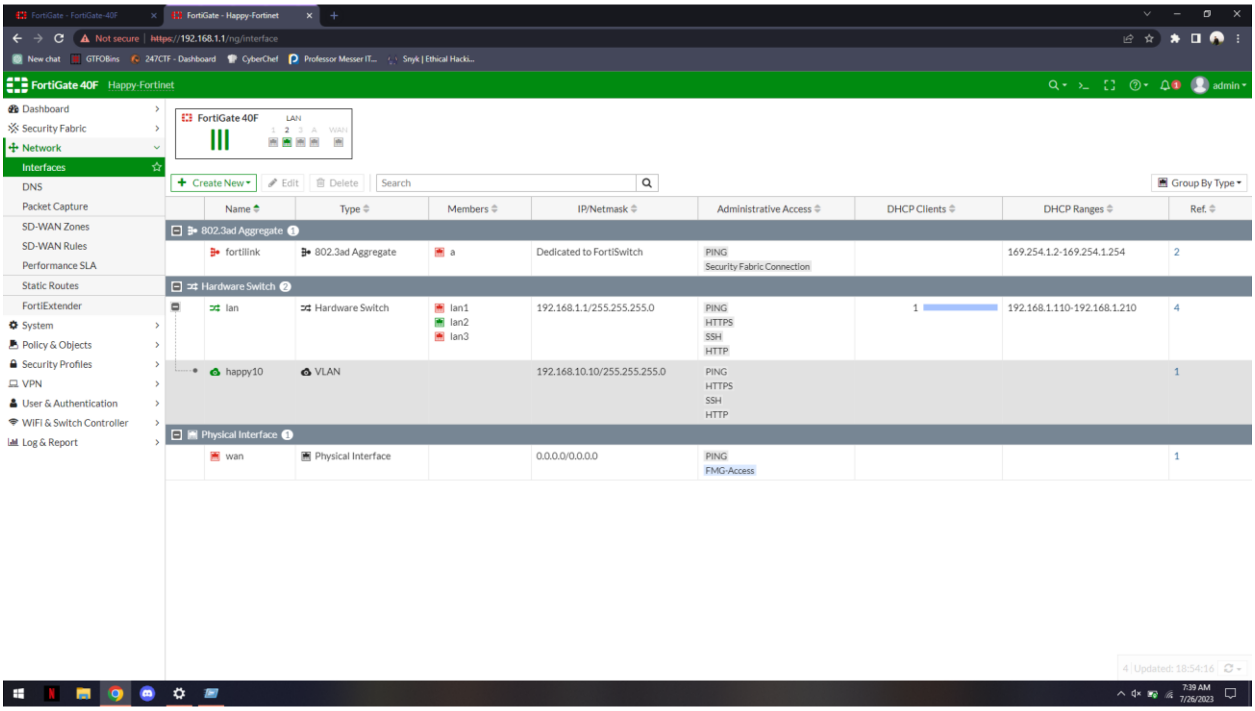
Device detection: ●
Security mode: ○

Traffic Shaping

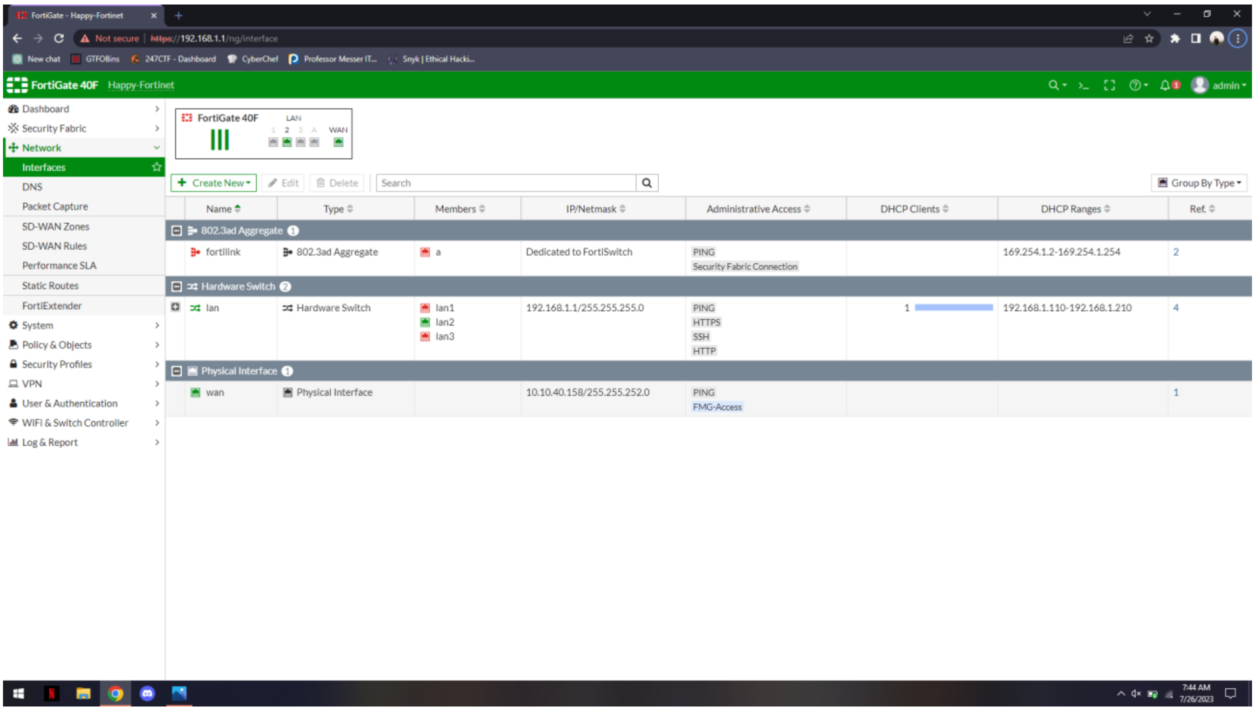
Outbound shaping profile: ○



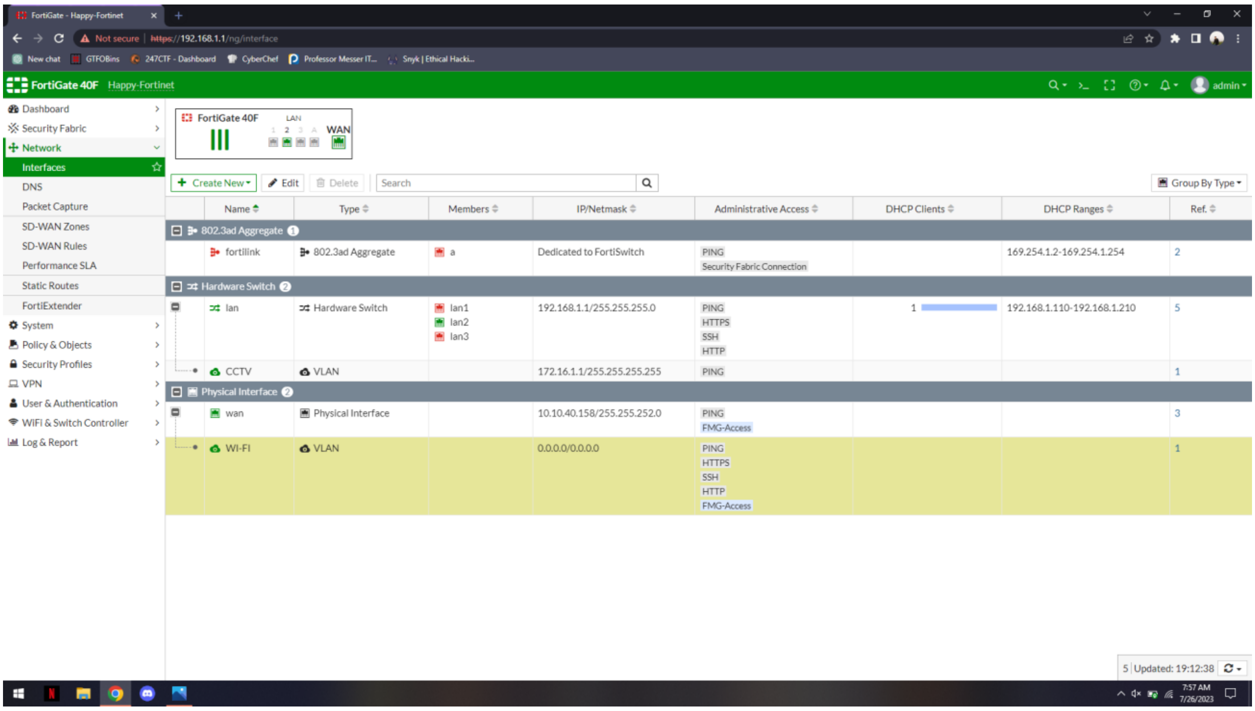
Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate	a	Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Hardware Switch 2							
lan	Hardware Switch	lan1 lan2 lan3	192.168.1.1/255.255.255.0	PING HTTPS SSH HTTP	1	192.168.1.110-192.168.1.210	4
Physical Interface 1							
wan	Physical Interface		0.0.0.0/0.0.0.0	PING FMG-Access			1



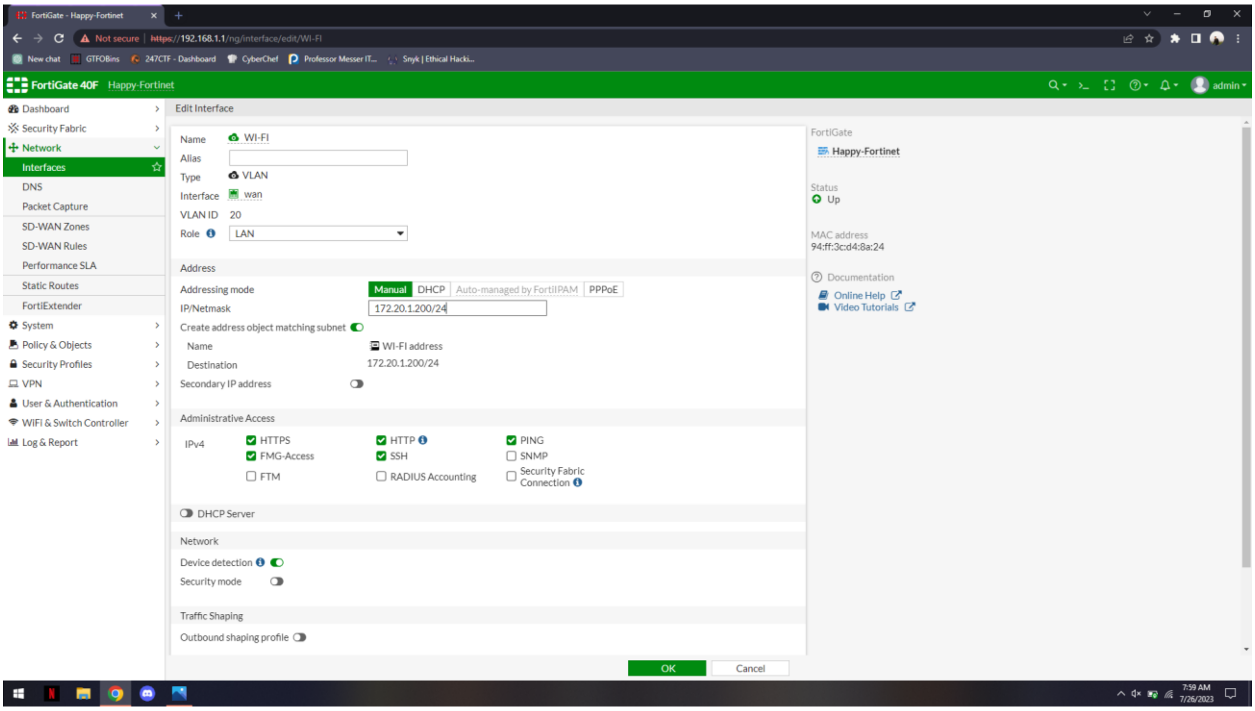
Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate	a	Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Hardware Switch 2							
lan	Hardware Switch	lan1 lan2 lan3	192.168.1.1/255.255.255.0	PING HTTPS SSH HTTP	1	192.168.1.110-192.168.1.210	4
happy10	VLAN		192.168.10.10/255.255.255.0	PING HTTPS SSH HTTP			1
Physical Interface 1							
wan	Physical Interface		0.0.0.0/0.0.0.0	PING FMG-Access			1



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate	a	Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Hardware Switch 2							
lan	Hardware Switch	lan1 lan2 lan3	192.168.1.1/255.255.255.0	PING HTTPS SSH HTTP	1	192.168.1.110-192.168.1.210	4
Physical Interface 1							
wan	Physical Interface		10.10.40.158/255.255.252.0	PING FMG-Access			1



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate	a	Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Hardware Switch 2							
lan	Hardware Switch	lan1 lan2 lan3	192.168.1.1/255.255.255.0	PING HTTPS SSH HTTP	1	192.168.1.110-192.168.1.210	5
CCTV	VLAN		172.16.1.1/255.255.255.255	PING			1
Physical Interface 2							
wan	Physical Interface		10.10.40.158/255.255.252.0	PING FMG-Access			3
WI-FI	VLAN		0.0.0.0/0.0.0.0	PING HTTPS SSH HTTP FMG-Access			1



Edit Interface

Name: WI-FI
Alias:
Type: VLAN
Interface: wan
VLAN ID: 20
Role: LAN

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by FortiIPAM PPPoE
IP/Netmask: 172.20.1.200/24
Create address object matching subnet: ●
Name: WI-FI address
Destination: 172.20.1.200/24
Secondary IP address: ○

Administrative Access

IPv4: ☑ HTTPS ☑ HTTP ☑ PING ☑ FMG-Access ☑ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection

○ DHCP Server

Network

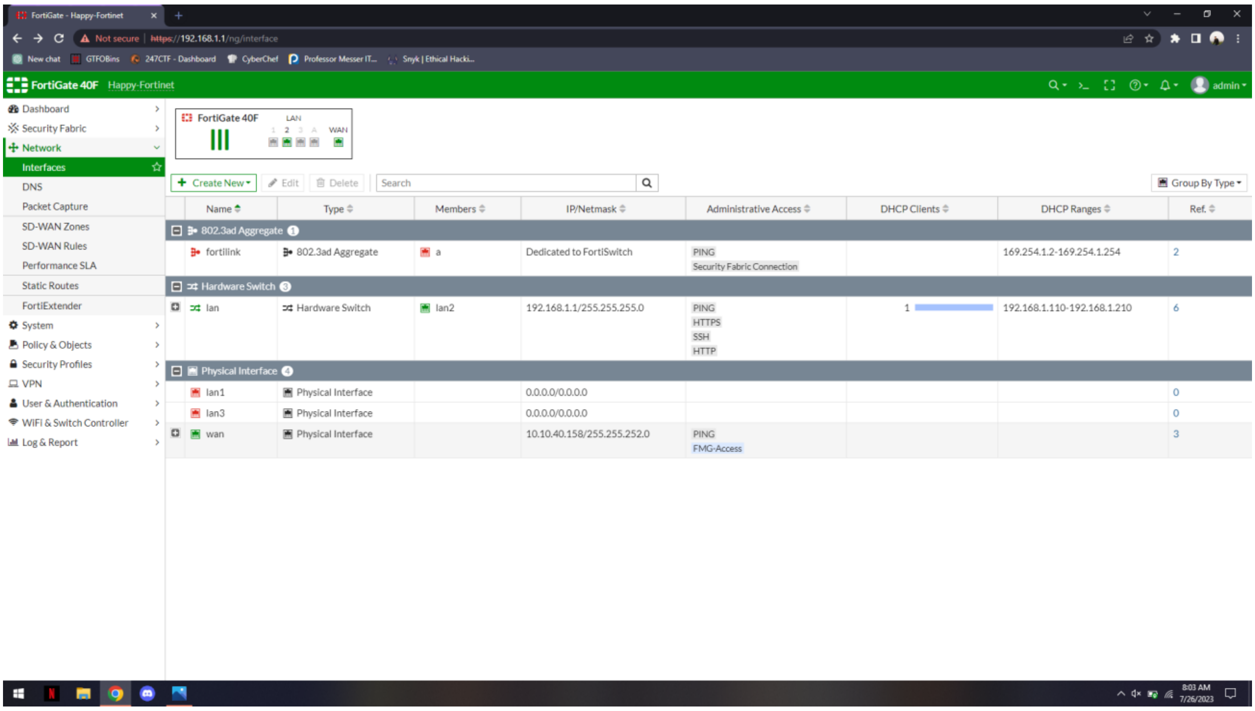
Device detection: ●
Security mode: ○

Traffic Shaping

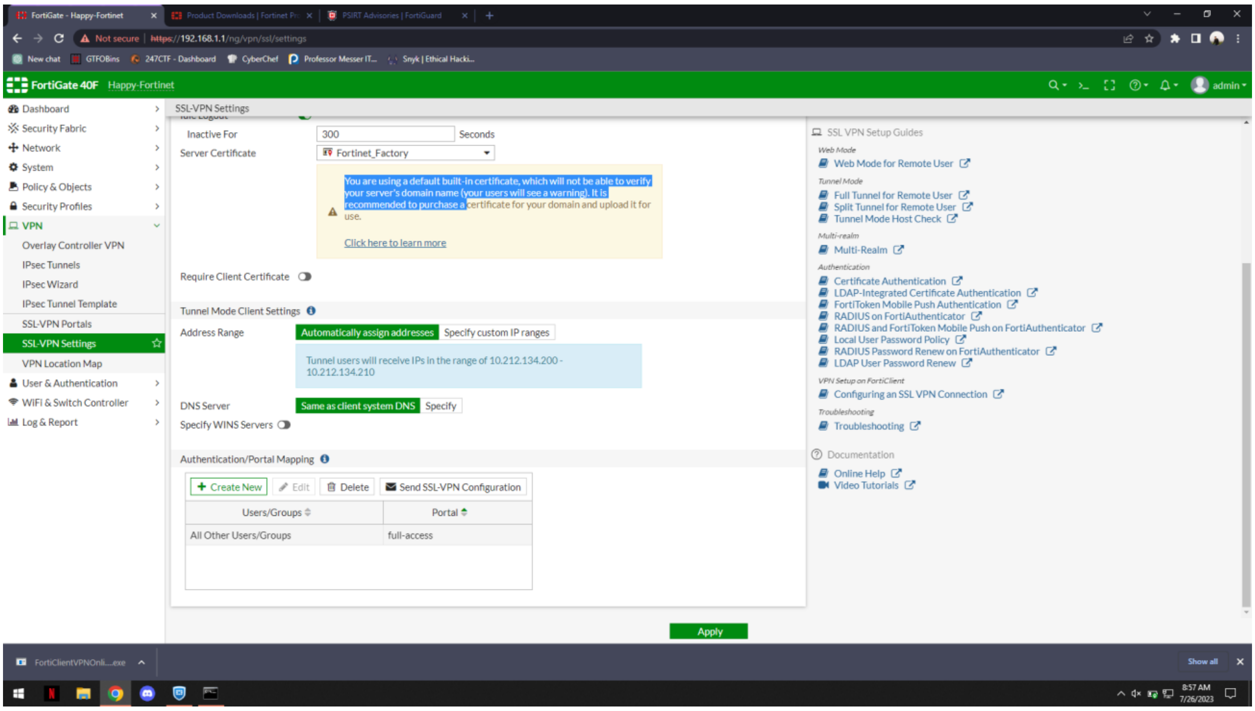
Outbound shaping profile: ○

FortiGate: Happy-Fortinet
Status: Up
MAC address: 94:ff:3c:d4:8a:24
Documentation: Online Help, Video Tutorials

OK Cancel



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate	a	Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Hardware Switch 3							
lan	Hardware Switch	lan2	192.168.1.1/255.255.255.0	PING HTTPS SSH HTTP	1	192.168.1.110-192.168.1.210	6
Physical Interface 4							
lan1	Physical Interface		0.0.0.0/0.0.0.0				0
lan3	Physical Interface		0.0.0.0/0.0.0.0				0
wan	Physical Interface		10.10.40.158/255.255.252.0	PING FMG-Access			3



FortiGate - Happy-Fortinet
Product Downloads | Fortinet Pr
PSIRT Advisories | FortiGuard
Not secure | https://192.168.1.1/ng/vpn/ssl/settings
FortiGate 40F Happy-Fortinet
Dashboard
Security Fabric
Network
System
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Authentication
WiFi & Switch Controller
Log & Report
SSL VPN Setup Guides
Web Mode for Remote User
Full Tunnel for Remote User
Split Tunnel for Remote User
Tunnel Mode Host Check
Multi-Realm
Certificate Authentication
LDAP-Integrated Certificate Authentication
FortiToken Mobile Push Authentication
RADIUS on FortiAuthenticator
RADIUS and FortiToken Mobile Push on FortiAuthenticator
Local User Password Policy
RADIUS Password Renew on FortiAuthenticator
LDAP User Password Renew
Configuring an SSL VPN Connection
Troubleshooting
Documentation
Online Help
Video Tutorials
Apply

SSL-VPN Settings

Inactive For: 300 Seconds

Server Certificate: Fortinet_Factory

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). It is recommended to purchase a certificate for your domain and upload it for use.

Click here to learn more

Require Client Certificate

Tunnel Mode Client Settings

Address Range: Automatically assign addresses | Specify custom IP ranges

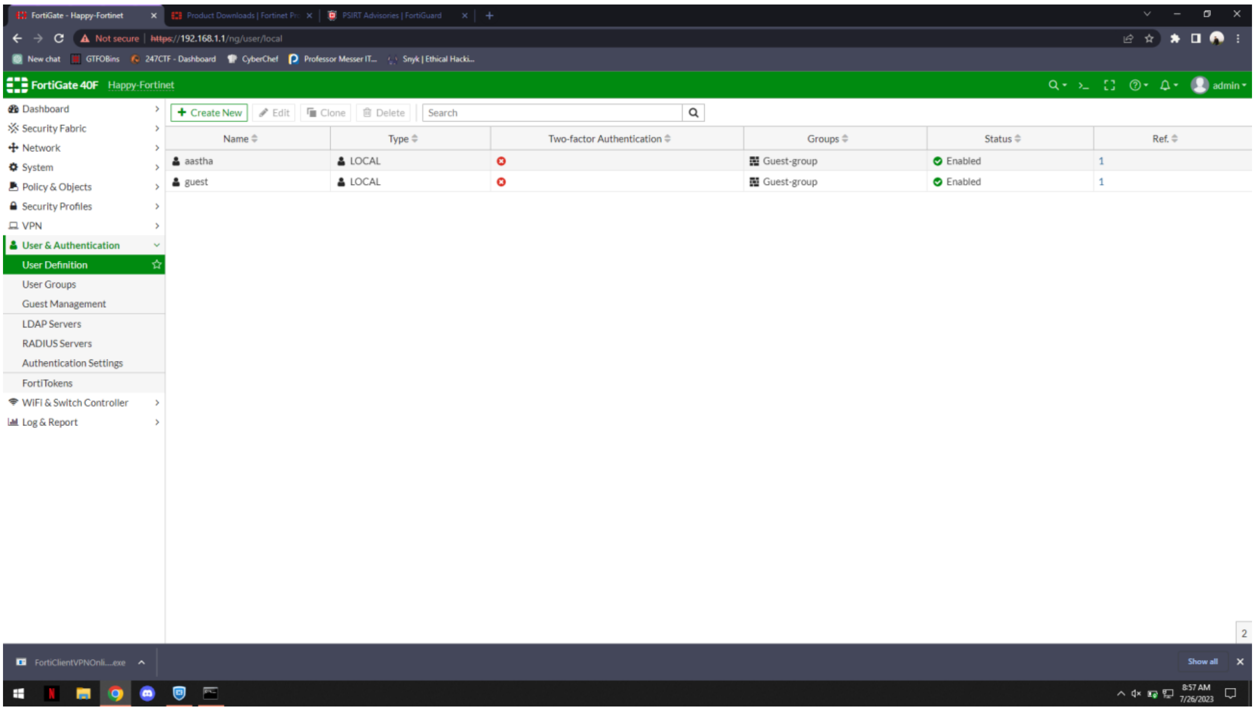
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server: Same as client system DNS | Specify

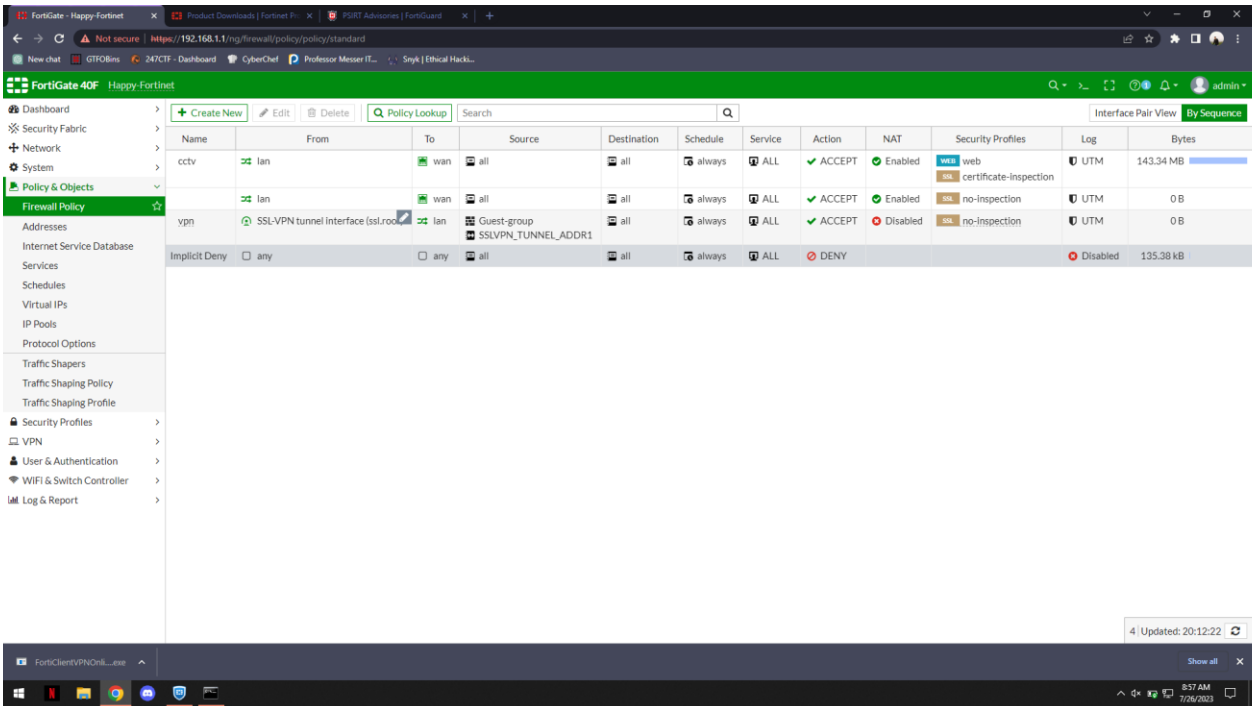
Specify WINS Servers

Authentication/Portal Mapping

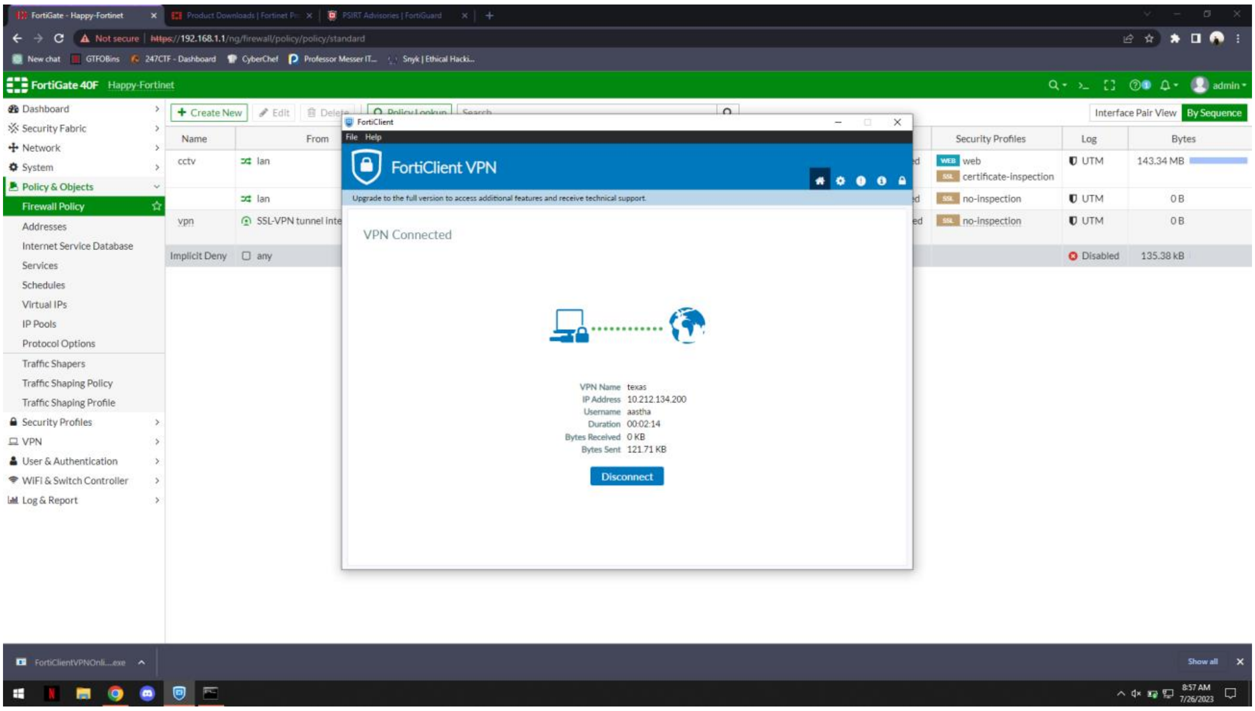
Users/Groups	Portal
All Other Users/Groups	full-access



Name	Type	Two-factor Authentication	Groups	Status	Ref.
aastha	LOCAL	✗	Guest-group	Enabled	1
guest	LOCAL	✗	Guest-group	Enabled	1



Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
cctv	lan	wan	all	all	always	ALL	✓ ACCEPT	Enabled	web certificate-inspection	UTM	143.34 MB
	lan	wan	all	all	always	ALL	✓ ACCEPT	Enabled	no-inspection	UTM	0 B
vpn	SSL-VPN tunnel interface (ssl.roo	lan	Guest-group SSLVPN_TUNNEL_ADDR1	all	always	ALL	✓ ACCEPT	Disabled	no-inspection	UTM	0 B
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	135.38 kB


FortiClient
File
Help
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
Disconnect

VPN Connected

VPN Name texas
IP Address 10.212.134.200
Username aastha
Duration 00:02:14
Bytes Received 0 KB
Bytes Sent 121.71 KB