FortiGate Essentials: A Comprehensive Guide for SMEs in Palestine

“Securing your digital frontier” Empowering SMEs

JULY 2, 2024
Arab American University
By: Samah Fayz Shammas
Supervisor: Dr. Mohammad Hamarsheh

Table of Contents

List of Figures

List of Abbreviations

APTs	Advanced Persistent Threats
DoS	Denial of Service
ESXi	Elastic Sky X integrated
FortiGate	A product of Fortinet Inc.
FTP	File Transfer Protocol
GUI	Graphical User Interface
HA clusters	High Availability clusters
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
LAN	Local Area Network
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NGFWs	Next Generation Firewalls
pfSense	Packet-filtering firewall and routing software
PPDIOO	Prepare, Plan, Design, Implement, Operate and Optimize
SD-WAN	Software-defined Wide Area Network
SPOF	Single Point of Failure
SPUs	Security Processing Units
SME	Small and Midsize Enterprise
SSL	Secure Sockets Layer
SYN flood	type of distributed denial-of-service
UTM	Unified Threat Management
VMware	Virtual Machine Software
VPN	Virtual Private Network
WAN	Wide Area Network

Abstract

This document offers an in-depth exploration of firewall technologies, specifically tailored for SMEs in Palestine, focusing on the critical role of FortiGate firewalls. It begins by tracing the evolution from traditional firewalls to sophisticated Next-Generation Firewalls (NGFWs) that incorporate machine learning, highlighting the significance of FortiGate in enhancing network security and mitigating risks through detailed case studies.

It then provides a methodical guide on selecting appropriate FortiGate models and configuring various aspects such as system interfaces, network settings, DHCP configurations, and static routing. The document further elaborates on policy creation, SD-WAN, IPv4 policies, and high availability setups, and covers essential aspects of regular maintenance, support, and training. It also includes detailed instructions for firmware updates, configuration backups, performance monitoring, and troubleshooting. Furthermore, it outlines available support resources and training opportunities to ensure that SMEs can maintain and optimize their FortiGate firewalls effectively.

Aiming to provide SMEs with a comprehensive strategy for deploying FortiGate firewalls to safeguard against cyber threats and ensure robust network security, this document provides all the necessary tools and knowledge for effective implementation and maintenance.

Acknowledgements

I would like to thank the people and organizations that helped me finish my senior project.

Dr. Mohammed Hamarsheh:
I am very grateful to Dr. Mohammed Hamarsheh, my supervisor, for helping me with this project and giving me valuable advice. His mentorship has been integral to its success.

Arab American University:
I would like to express my gratitude to the Arab American University for providing a stimulating academic environment and the essential tools that helped facilitate the completion of this project.

My Family:
My family, whose unwavering support and encouragement have been the driving force behind my academic pursuits. Their belief in my capabilities has been a constant source of motivation.

Friends and Peers:
I would like to express my appreciation to my friends and peers, whose camaraderie and shared experiences have added depth and joy to my academic journey.

Sincerely,
Samah Shammas

1 Introduction

1.1 Introduction and Motivation

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.
(Schneider, 2000)[1])

In an era dominated by the relentless expansion of cyber threats, establishing robust network security policies has become an absolute necessity for organizations of all sizes. A proactive and effective defense mechanism to safeguard sensitive data and ensure the uninterrupted functioning of organizational networks is required. In Palestine, larger companies and organizations use commercially available firewall solutions routinely, this is not the case for small-medium enterprises and organizations SMEs)[2] Nevertheless, exposure to cyber threats does not depend on the size of the organization. Not having an adequate cyber defense mechanism can lead to substantial losses for a company or organization up to bankruptcy. The motivation of this project is to improve the defense for SMEs in Palestine by providing easy to implement guidelines. Companies like Fortinet, Cisco, and Palo Alto provide commercial firewall solutions. The most used firewall solution in Palestine is FortiGate from Fortinet, which is why this project focuses on this product.

This manual will help SMEs understand the dangers of cyber threats and how to protect themselves effectively. The guidelines will enable individuals to establish a firewall independently, without the requirement for extensive knowledge of the topic.

1.2 Aims and objectives

The **aim** of this manual is to address the basic policies of firewalls with focus on FortiGate. It highlights the importance of policies and provides a practical guidelines for IT specialists working in SMEs in Palestine. The easy-to-use manual can be used to

[1] Schneider, B. (2000). Secrets & Lies, John Wiley & Sons.

[2] SMEs – defined as the enterprises that employ a maximum of 25 people and have an annual turnover of no more than $7 million - make up 95% of the Palestinian economy. (Source: Palestine Money Authority, https://www.pma.ps/en/ [Accessed January 17, 2024].

enhance the security systems of organizational networks. Applying the policies will ensure the robust application of essential security measures.

The following **objectives** are defined to achieve this aim:

- This manual aims to enhance network security for SMEs in Palestine by providing a country and needs-based solution.
- The primary emphasis is on practical processes that facilitate the implementation of FortiGate, even in the absence of adequate resources or FortiGate expertise.
- Policies for firewalls are explained and defined, including configuration of the Wide Area Network (WAN) and Local Area Network (LAN).
- Key aspects such as SD-WAN integration, IPv4 policies, IPv4 Denial of Service (DoS) policies, Site-to-Site Virtual Private Network (VPN) configurations, and the implementation of Virtual IP Network Address Translation (NAT) are addressed.
- The manual will help SMEs by providing them a straightforward guide to set up FortiGate firewalls. Existing instructions, and training sites will be incorporated into the guidelines.

1.3 Problem Statement

This project aims to address the issue of inadequate understanding and implementation of effective FortiGate firewall policies, a challenge that hinders organizations from fortifying their networks against cyber threats. The problem goes beyond theoretical knowledge, involving difficulties in configuring and customizing policies to align with specific organizational needs. Furthermore, the dynamic nature of cyber threats increases the risk, as there is a lack of clarity on how to adapt FortiGate configurations to evolving security challenges. Resource constraints further compound the problem, limiting the accessibility of robust security measures. In essence, the identified problem is a crucial obstacle for organizations trying to establish resilient network defenses in the face of evolving cyber threats and advanced persistent threats (APTs).

1.4 Document Structure

The remainder of this document is organized into three major sections:

- **Section 2: Background**

This section provides an overview of the evolution of firewall technologies, starting from the first generation of packet filtering firewalls developed in 1988 to the current Next Generation Firewalls (NGFWs) with machine learning capabilities. It also discusses the concept of Unified Threat Management (UTM) and the features of FortiGate firewalls. Additionally, it addresses the risks and attack scenarios associated with firewall misconfigurations

- **Section 3: Implementation**

This section provides guidance on selecting the most suitable FortiGate model based on the size and specific requirements of the SME. It includes a model selection guide, a cost-benefit analysis, and detailed descriptions of various FortiGate models tailored for different organizational needs. Following the selection, it provides comprehensive instructions for the initial setup and configuration of FortiGate devices. It covers unboxing, physical setup, network connection, and accessing the FortiGate interface. It also includes detailed steps for WAN and LAN configuration to ensure secure and efficient network operations. The section further discusses the creation and implementation of various security policies on FortiGate firewalls, including basic and advanced IPv4 policies, configuring Software-defined Wide Area Network (SD-WAN), implementing Denial of Service (DoS) policies, Virtual Private Network (VPN) configurations, and Network Address Translation (NAT) with Virtual IPs.

- **Section 4: Regular Maintenance, Support, and Training**

This section provides an overview of the regular maintenance and support required to keep FortiGate firewalls functioning optimally. It lists factors to consider for firmware updates, troubleshooting common issues, and accessing FortiGate support resources. Additionally, it includes recommendations for ongoing training and the use of interactive learning modules to enhance understanding and implementation of security measures.

By following the detailed guidance provided in these sections, SMEs in Palestine can significantly enhance their network security, ensuring robust protection against cyber threats and maintaining the integrity of their business operations.

2 Background

2.1 Overview

The first generation of firewalls was the packet filtering firewall, developed by Digital Equipment Cooperation (DEC) in 1988. It was designed to protect the network against unwanted packets from certain source IP addresses and was not aimed at detecting viruses or network threats. In 1990, AT&T Bell Labs developed the stateful firewall to make packet filtering networks more efficient. DEC developed the application-gateway firewall in 1991 to detect network attacks. The web application firewall was introduced in 1997 to protect web servers and was successful in detecting network attacks. In 2004, the concept of Unified Threat Management (UTM) was introduced to combine every type of firewall into one machine. This concept evolved into NGFW in 2009, which became the most popular choice for defending industrial and enterprise networks, especially when combined with machine learning and other advanced intrusion detection techniques. Today, there are many companies offering firewalls at different levels. The most advanced companies in this field are Fortinet, Cisco, and Palo Alto. All three companies have good products which are comparable. Figure 1 shows the timeline of these developments. Comparing the three solutions would be a project by itself. Because The Arab American University uses FortiGate and secondly, it is the most frequently used solution in the West Bank, this project will use FortiGate tools. The next paragraphs will explain the evolution in more detail.

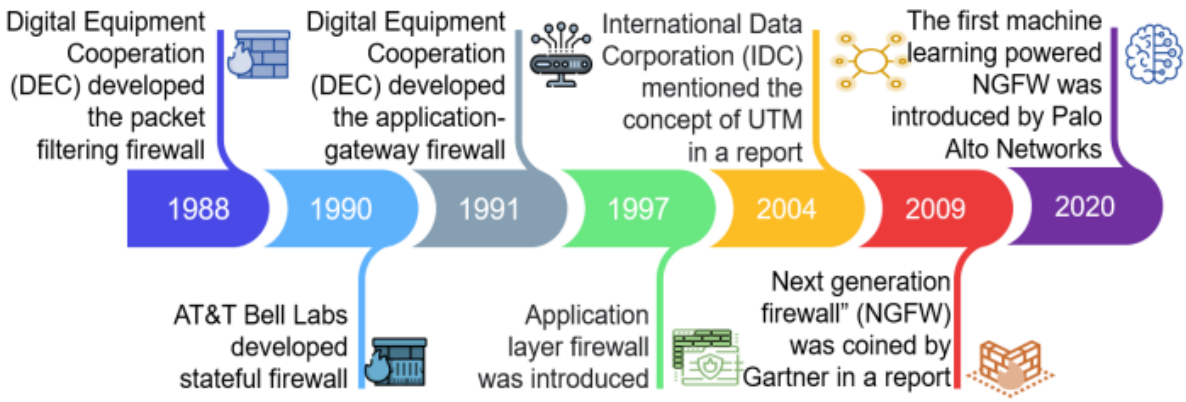


Figure1: Firewall evolution map[3]

[3] Liang, J. / Kim, Y. (2022). Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall, IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)

2.2 Evolution of Firewall Technologies

It is important to understand the technological evolution to make recommendations on how to use firewalls. From early firewalls to Next Generation Firewalls (NGFWs) with machine learning, network security has changed a lot.

As the Internet and the Digital Economy have expanded, firewalls have consistently evolved to serve as crucial security appliances. Firewalls have changed a lot over time. They used to be just software tools, but now they are hardware devices that can be used in private and public cloud environments. This changes how cybersecurity is done, from dealing with random threats to fighting sophisticated attacks by countries and cybercriminals. Firewalls have changed in form, function, speed, and security features. The first firewalls were simple and based on rules. Later, there was a newer version that had more features but did not work well together. The invention of NGFW changed how we protect ourselves by using tools that use apps, who uses them, and what they see. This helps us control and find out about advanced attacks. Now, NGFW with machine learning is used to provide real-time, inline zero-day protection, device visibility, and behavioral anomaly detection. As networks become more connected, firewalls will need to change even more. They need to combine different solutions into one system and use advanced technology to predict and respond faster to threats. In this changing cybersecurity landscape, it is important for those who want to not just survive, but to thrive in the digital era to be able to innovate and use fast firewall technologies. The next paragraphs will explain the evolution with the help of Figures.

2.2.1 First Generation – Early Firewalls

Early firewalls were simple and focused on checking and filtering packets sent into a network or system. Stateful filters were used to keep track of connections between computers to judge packets. These firewalls were straightforward to operate and manage. However, they were reactive and based on rules, which made them easily defeated.

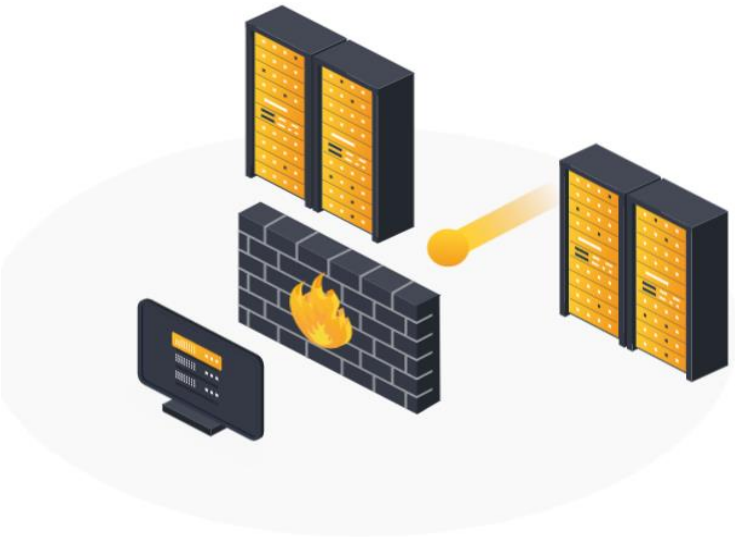


Figure 2: First Generation of Firewalls[4]

2.2.2 Second Generation – Unified Threat Management

The second generation of firewalls was made because people started using more applications in the 2000s. These firewalls have protection against viruses and other harmful things. They also check what people send and receive online, filter out bad stuff using web proxies, connect offices that are far away using VPNs, and block spam. They had more capabilities and better protection than the early firewalls. However, there was a lack of integration between each function, which led to security gaps, poor performance, and complex policy management.

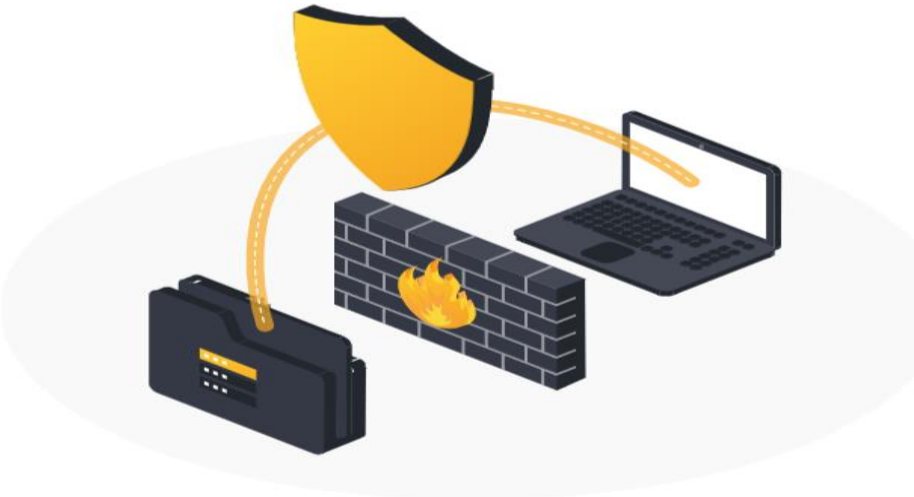


Figure 3: Second Generation of Firewalls[4]

[4] Palo Alto, The Evolution of Firewalls, https://www.paloaltonetworks.com/resources/infographics/the-evolution-of-firewalls [Accessed January 18, 2024]

2.2.3 Third Generation – Next Generation Firewalls

The first Next-Generation Firewall (NGFW) was introduced in 2008. The NGFW is built around integrated capabilities that use awareness of apps, user identity, and content to offer enhanced application visibility and control. It supports secure, encrypted traffic via SSL/TLS and detects and prevents advanced attacks by identifying evasive techniques and automatically counteracting them.

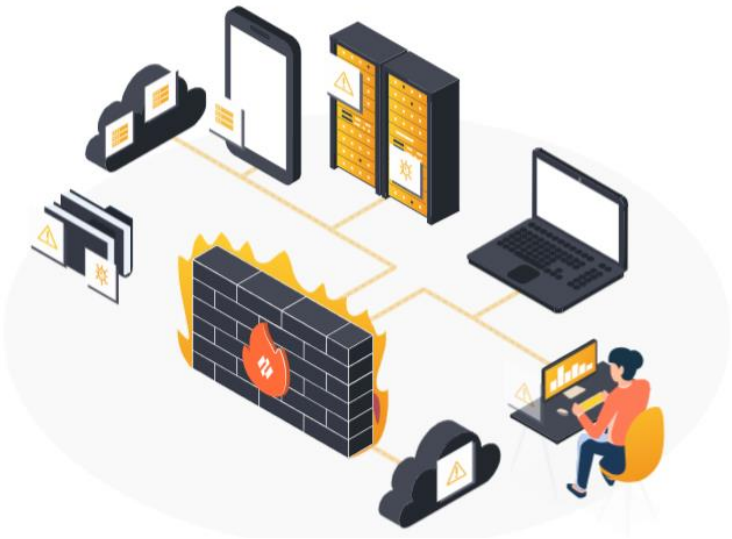


Figure 4: New Generation of Firewalls[4]

2.2.4 Proactive NGFWs with Machine Learning

Machine learning has enabled Next-Generation Firewalls (NGFWs) to deliver proactive, real-time, and inline zero-day protection. NGFWs can identify variants of known attacks as well as many unknown cyberthreats. They provide complete device visibility, behavioral anomaly detection, and native enforcement to secure Internet of Things (IoT) devices without the need for additional sensors or infrastructure. NGFWs also serve up recommendations for policy improvements.

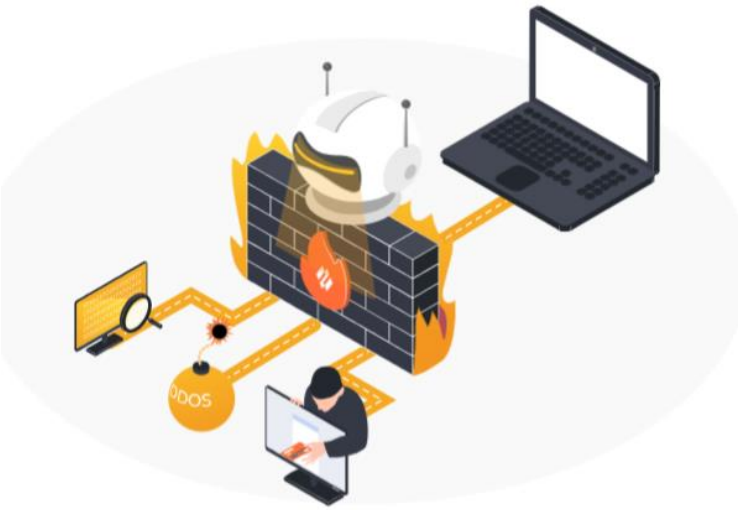


Figure 5: NGFWs with Machine Learning[4]

Drawing parallels to this evolution, FortiGate stands out as a Unified Threat Management solution, consolidating security functions and offering a single management console for ease of administration and consistent updates.

2.3 FortiGate Essentials, components and features

Fortinet's firewall solution, FortiGate, is a comprehensive line of network appliances, implementing a UTM approach. These appliances integrate networking and security features, providing services at layers 2 and 3, network security services, and application security services. The consolidated approach ensures efficient security management and updates across all devices involved in UTM.

2.3.1 FortiGate components and features overview

FortiGate comprises specialized hardware models running the FortiOS operating system. Key components include dedicated Security Processing Units (SPUs) for accelerated security tasks. The firewall offers core functionalities like stateful packet inspection, alongside Virtual Private Network (VPN) support for secure communication.

It incorporates features such as an Intrusion Prevention System (IPS), antivirus, web filtering, and application control to safeguard networks from various threats. FortiGate enables Secure Sockets Layer (SSL) inspection to uncover hidden threats in encrypted

traffic and supports multiple user authentication methods. Robust logging, reporting, and High Availability (HA) configurations enhance network monitoring and resilience. The firewall's scalability and versatility make it suitable for diverse organizational security needs.

2.3.2 Risks and attacks scenarios of the misconfigurations

Without implementing essential configurations and policies on firewalls, such as WAN and LAN settings, security policies, VPN configurations, and Virtual IP NAT configurations, organizations expose themselves to various vulnerabilities. Attackers can exploit these lapses in different ways.

- **Unprotected Interfaces:**

Attack Vector: Absence of WAN and LAN configurations leaves interfaces unprotected, enabling unauthorized access and potential network infiltration.
Misuse Scenario: Attackers may exploit this vulnerability to gain unauthorized access to internal resources, compromise sensitive data, or launch lateral movement attacks.

- **Unrestricted Traffic Flow:**

Attack Vector: Without properly configured security policies, there is a lack of traffic control mechanisms between WAN and LAN, allowing unmonitored data flow.
Misuse Scenario: Attackers could exploit this situation to conduct reconnaissance, propagate malware, or execute other malicious activities unnoticed.

- **DoS Vulnerability:**

Attack Vector: Failure to set up DoS policies exposes the network to DoS attacks, potentially overwhelming resources.
Misuse Scenario: Attackers might launch DoS attacks, causing service disruptions, network downtime, and creating opportunities for further exploitation.

- **Insecure VPN Connections:**

Attack Vector: Improper site-to-site VPN configurations can lead to insecure connections, potentially exposing sensitive information during data transmission.

Misuse Scenario: Attackers may intercept or manipulate data in transit, leading to data breaches, unauthorized access, or even network compromise.

- **NAT Misconfigurations:**

Attack Vector: Virtual IP NAT configurations are crucial for proper translation between LAN and WAN, and their absence can lead to misrouting or exposure of internal IPs.
Misuse Scenario: Attackers could exploit misconfigurations to bypass security controls, launch man-in-the-middle attacks, or gain insights into internal network structures.
Itis important to know how to configure these policies in the right way. For example, the following figure shows two examples of a DoS attack log on UDP flood, and the action taken by FortiGate according to the configured actions.

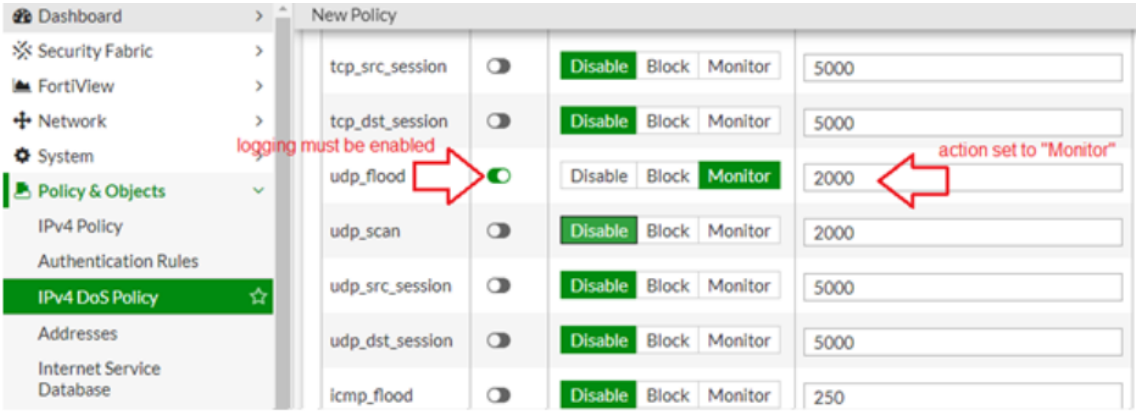


Figure 6: DoS Policy enabled as "Monitor"[5]

And the log action will be showing 'detected' as highlighted below since action set to monitor only.

[5] Fortinet Community https://community.fortinet.com/t5/FortiGate/Technical-Tip-DoS-attack-log-according-to-action-set-on-DoS/ta-p/198465 [Accessed January 18, 2024].

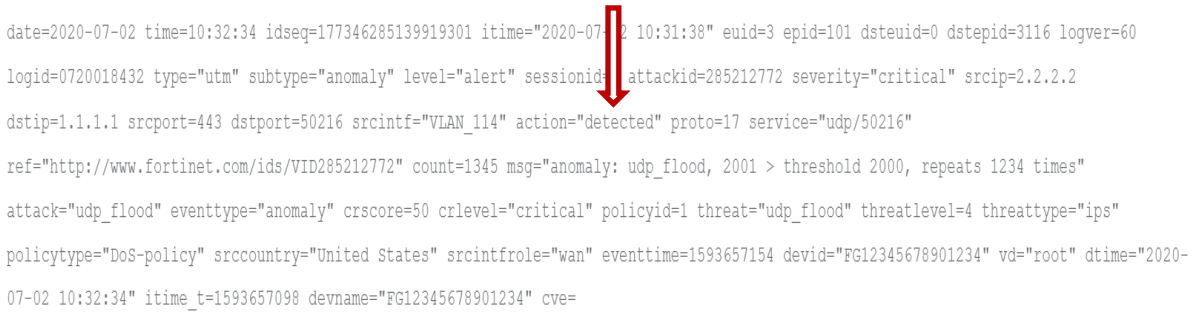


Figure 7: The log's action "Detected" [5]

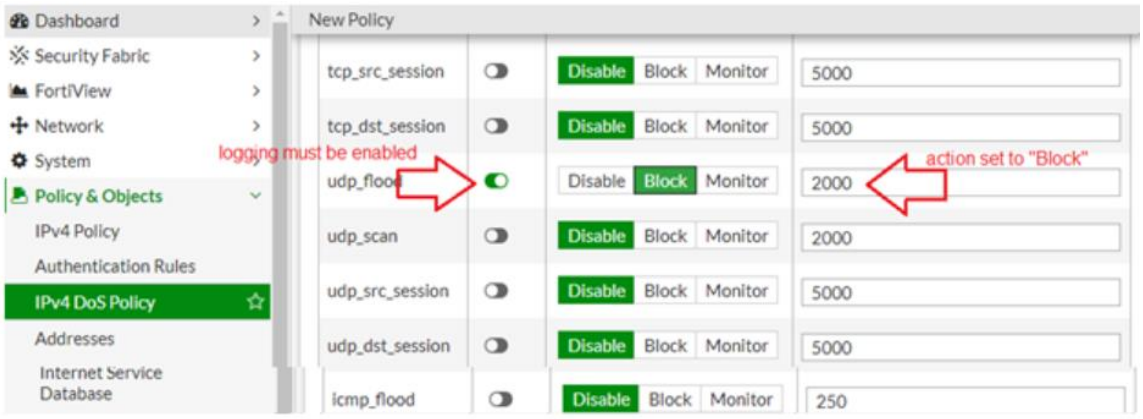


Figure 8: DoS Policy enabled as "Block"[5]

The log 's action will be showing "clear_session" as highlighted below since action set to "Block".

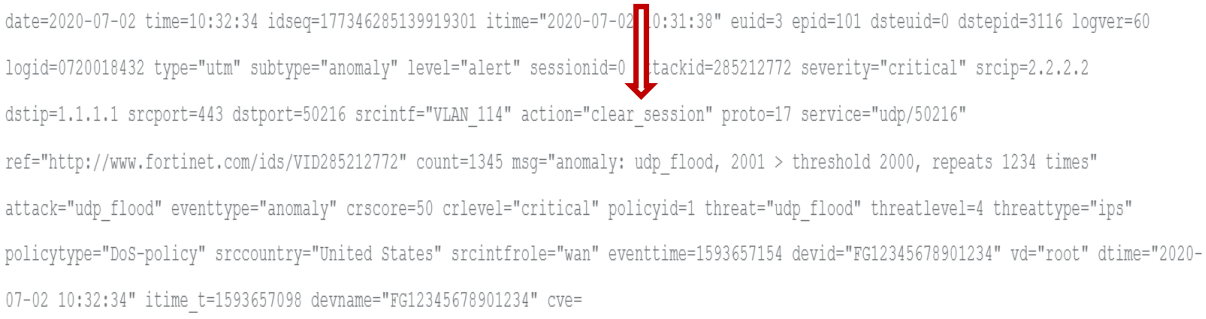


Figure 9: The log's action "Clear session"[5]

3 Implementation

3.1 Introduction

Setting up effective security policies with FortiGate can be a real challenge for those with limited knowlege and limited access to resources. This methodology chapter is designed as a step-by-step guide, specifically for individuals and Palestinian IT specialists working in SME's who may struggle with the basics of FortiGate policies.

Understanding the challenges faced by those with limited experience or constrained resources is important to start with. This guide aims to make the learning curve more manageable. This chapter will break down the process of establishing FortiGate policies into easy-to-follow steps. This methodology provides clear instructions to help grasp and apply the essentials of FortiGate policies.

3.2 Choosing the Right FortiGate Model

Choosing the right FortiGate model depends on several factors, such as the size of the organization, the number of users, the type and volume of network traffic, and specific security requirements. Here's a guide to help you select the appropriate FortiGate model:

1. **Assess Your Network Needs:**
    - **Number of Users:** Determine the number of users who will be accessing the network.
    - **Network Traffic:** Estimate the volume of network traffic, including peak usage times.
    - **Security Requirements:** Identify specific security needs such as VPN, IPS, web filtering, and application control.
    - **Growth Potential**: Consider future growth and scalability needs.

2. **Match Your Needs with FortiGate Models:**
    - **Small Businesses:** Small businesses typically have fewer users and less network traffic, but still require robust security features, even if they have fewer users and less network traffic.
    - **Medium-Sized Businesses:** These businesses need more advanced security features to handle bigger user bases and increased network traffic.

3.2.1 FortiGate models

There are many different FortiGate models ranging from entry level hardware appliances to high end appliances. FortiGate VM, a virtual appliance offers the same protection as the physical appliances. This ensures that FortiGate can fit seamlessly into various environments.

Fortinet offers a variety of FortiGate models to cater to different network sizes and requirements. The following section describes the various FortiGate models based on the size of organizations and their typical use cases:

1. **Small to Medium-sized Businesses (SMBs):**
    - FortiGate 30E: Suitable for small offices or businesses with basic security needs.
    - FortiGate 50E: Ideal for small to medium-sized businesses with moderate network traffic.

The FortiGate/FortiWiFi 50E series provides an application-centric, scalable, and secure SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses.

Figure 10: FortiGate 50E device[6]

[6] Fortinet Product Infos https://www.fortinet.com/ [Accessed January 25, 2024]

2. **Medium to Large-sized Enterprises:**
    - FortiGate 100E: Designed

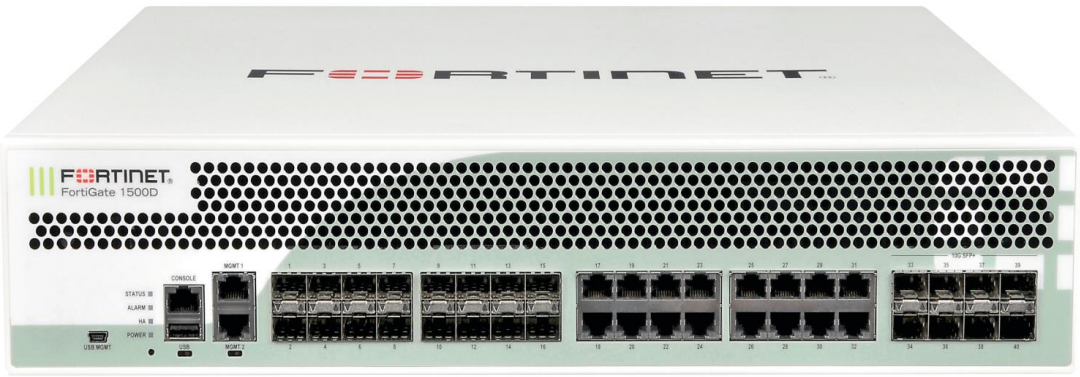


Figure 11: FortiGate 1500D device[6]

3. **Enterprise and Data Centers:**
    - FortiGate 500E: Suitable for larger enterprises and data center environments with high-performance requirements.
    - FortiGate 600E: Offers increased throughput and advanced security features.
    - FortiGate 800E: Designed for large enterprises with demanding security and performance needs.

4. **Next-Generation Firewall (NGFW) Series:**
    - FortiGate 3000 Series: Focuses on advanced threat protection and security features for organizations requiring a robust NGFW solution.
    - FortiGate 5000 Series: Offers high-performance next-gen firewall capabilities for large enterprises and service providers.

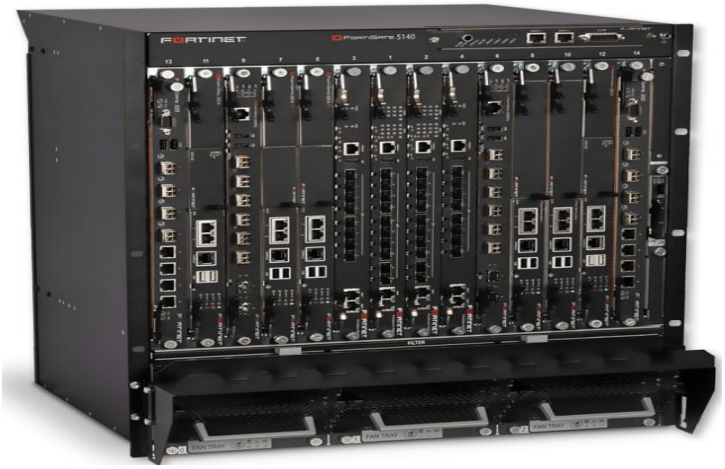


Figure 12: FortiGate 5000 device[6]

5. Secure SD-WAN Appliances:

1) FortiGate 60F: A versatile solution suitable for distributed enterprises requiring secure SD-WAN functionality.

Figure 13: FortiGate 60F device[6]

2) FortiGate 100F: Provides increased performance for larger SD-WAN deployments.

Featured FortiGate Models for Small Businesses

Model	Users	Throughput (Mbps)	Key Features
FortiGate 30E	1-10	950	Basic firewall protection, VPN, application control, web filtering, antivirus
FortiGate 50E	10-25	2500	Enhanced security features, VPN, IPS, web filtering, application control, compact and fanless design
FortiGate 60F	10-30	10,000	High performance, secure SD-WAN, application control, web filtering, IPS, antivirus

Featured FortiGate Models for Medium-Sized Businesses

Model	Users	Throughput (Mbps)	Key Features
FortiGate 100E	25-50	7,400	High performance, VPN, IPS, application control, web filtering, secure SD-WAN
FortiGate 200E	50-100	21,000	Advanced security features, high throughput, VPN, IPS, application control, secure SD-WAN, HA support
FortiGate 300F	100-200	30,000	Very high performance, advanced threat protection, VPN, IPS, application control, HA support, robust logging and reporting

3.3 FortiGate Policies and Starting Guide

Selecting the appropriate FortiGate model is the first step in enhancing network security for SMEs in Palestine. Once the right model is chosen, the next critical step involves establishing robust firewall policies. These policies ensure that only authorized traffic is allowed, while also blocking potentially harmful data.

Types of Policies:

1. **Based on IP Addresses and Protocols:**
   - Allow only necessary IP protocols (e.g., ICMP, TCP, UDP) and restrict them to specific hosts and networks.
   - Block traffic with invalid or private IP addresses.
2. **Application-Specific Policies:**
   - Use application firewalls or proxies to validate and filter incoming traffic before it reaches internal servers.
   - Employ outbound application proxies, such as HTTP proxies, to filter dangerous content and log web traffic.
3. **User Identity Policies:**
   - Enforce user identity policies using VPNs and network access control (NAC). Log user identities in firewall logs.
4. **Network Activity Policies:**
   - Implement policies to block inactive connections after a specified period.
   - Use traffic throttling or redirection policies to manage high rates of traffic, ensuring critical traffic is prioritized.

3.4 Basic Settings

When starting with an organization's network setup, it is crucial to get the basics right in FortiGate. This involves creating configurations, using CLI commands, setting up IP access, configuring DHCP, and being able to restore configurations from backups.

In this section the following aspects will be discussed: WAN and LAN setup, including SD-WAN, and establish security policies like IPv4 and DoS configurations. Next is VPN site-to-site setup and Virtual IP NAT configuration for managing network traffic.
To keep the system running smoothly, monitoring and maintenance, including firmware updates and backup procedures is important. This quick guide is your go-to reference for setting up essential configurations and ensuring a secure network environment with FortiGate.

Configuration Steps:

- **WAN/LAN Configuration**: Set up WAN and LAN interfaces, including IP address settings and DHCP server configuration.
- **IPv4 Policies:** Create and apply policies to control traffic between different network zones, including basic and advanced security measures.
- **SD-WAN Integration:** Configure SD-WAN to improve WAN performance and reliability.
- **DoS Policies:** Implement Denial of Service (DoS) policies to protect against attacks.
- **VPN Configurations:** Set up Site-to-Site and Remote Access VPNs for secure communication.
- **NAT with Virtual IPs**: Configure Network Address Translation (NAT) using Virtual IPs to manage traffic between internal and external networks.

3.4.1 Adjust FortiGate VM settings

To work in FortiGate's network security environment, a physical or virtual appliance is required. The flexibility of the VMware Workstation will be used to demonstrate the previously discussed points. Using this virtualization platform is used to execute essential configurations and commands to establish connectivity and assign a specific IP address through the FortiGate Command Line Interface (CLI). This process enables seamless interaction with the FortiGate web interface, empowering users to implement and fine-tune security measures efficiently.

Setup your VMware and try to connect to FortiGate through Web.

1. **Download VMware workstation from the VMware official website and finish the setup.**

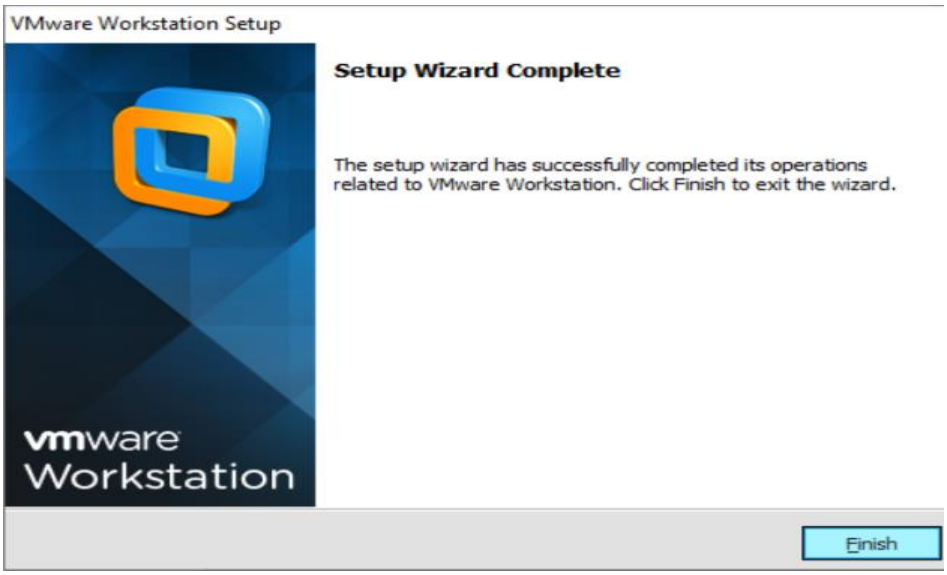


Figure -14: VMware workstation download[7]

2. **Get The ISO image of FG VM:**
   - → Go to https://support.fortinet.com/ and create an account.
   - → Then, click on the support button and choose VM images.
   - → select the platform, which is VMware ESXi, please make sure to download a new deployment called FortiGate VMware not FortiFirewall, to avoid errors during the configurations.

[7] FortiGate https://support.fortinet.com/welcome/#/ [Accessed February 1, 2024]

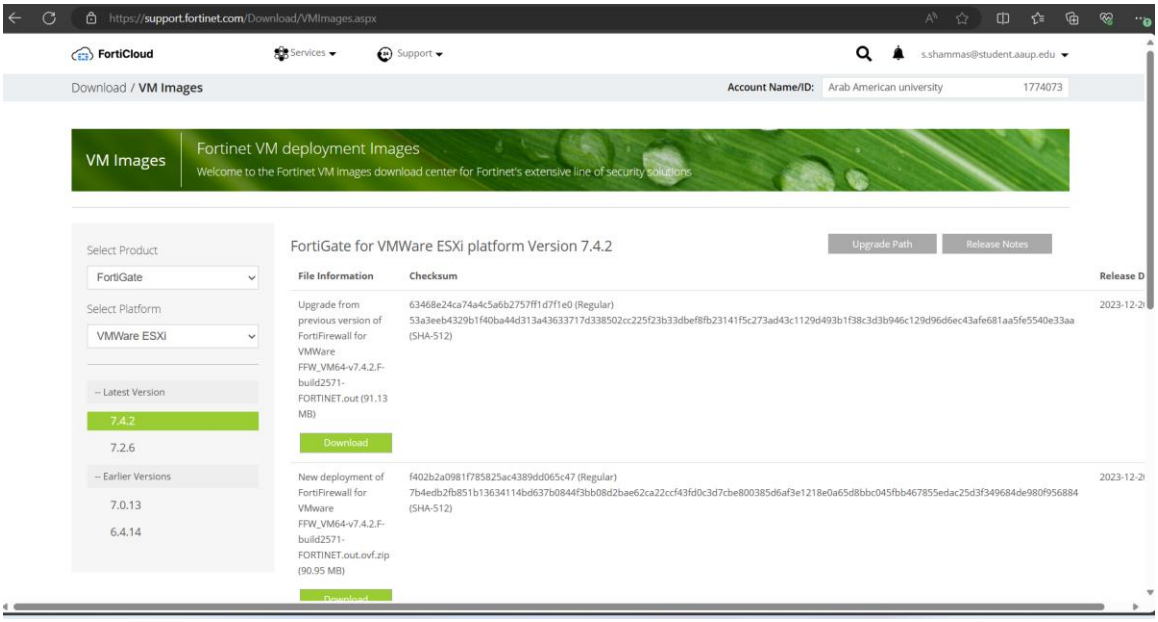


Figure 15: Download FG VM ISO image[7]

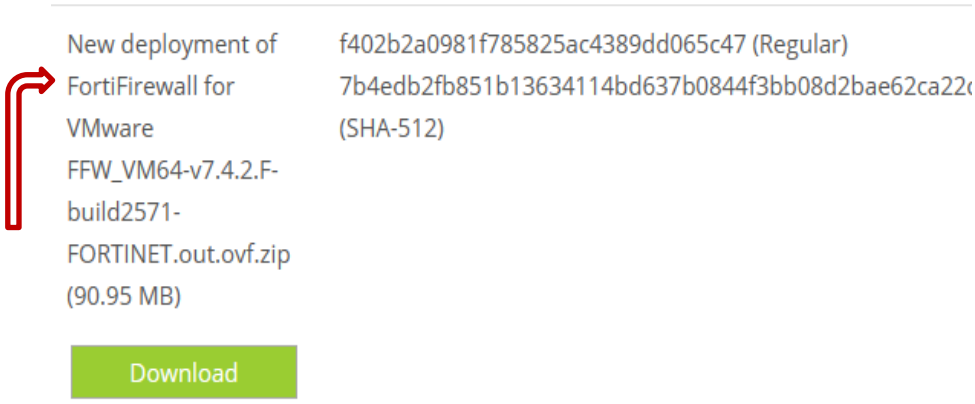


Figure 16: New deployment of FortiFirewall vs. FortiGate[7]

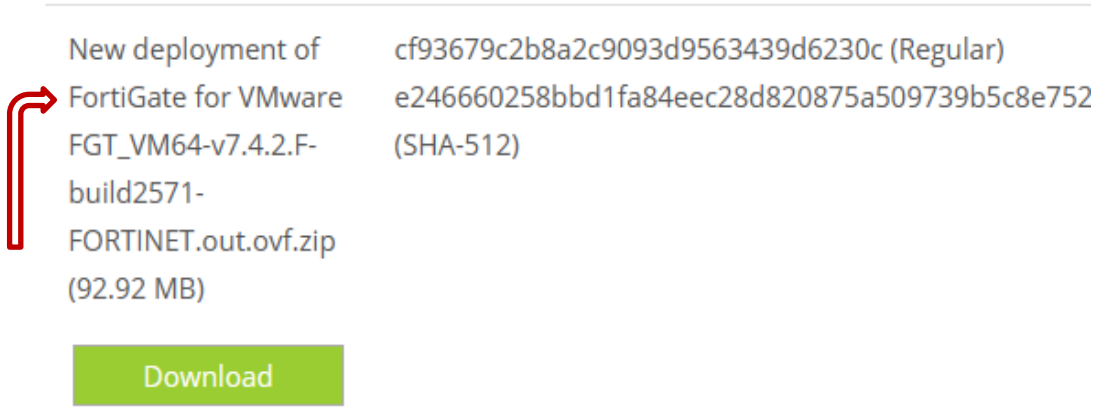


Figure 17: Deployment of FortiFirewall vs. deployment of FortiGate[7]

3. Import FortiGate with VMware and start the configurations

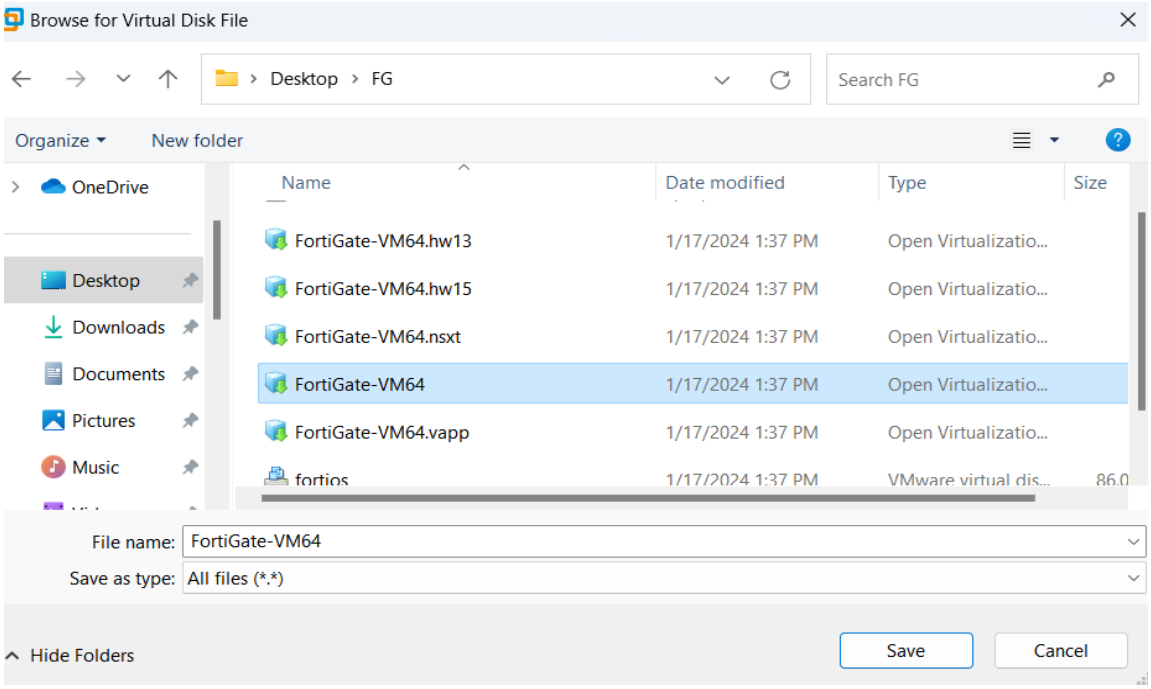


Figure 18: Import the iso image with VMware[7]

The last step is to modify the network adapters:

→ Click on Network adapter, make sure the network connection is set to bridged, connected directly to the physical network. This means this virtual machine will be a member of your physical network. You can ping an access to this virtual machine from the physical computer. The bridge network adapter would act as the interface to the Internet.

→ Click on network adapter two. This would be LAN interface or internal network. Select the LAN segment.

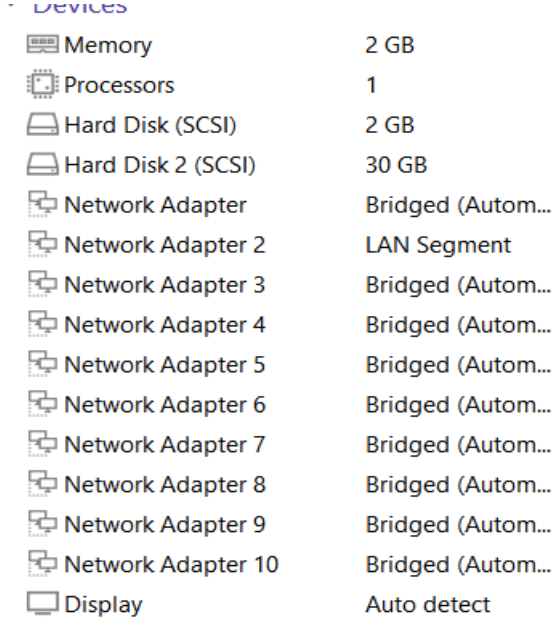


Figure 19: Bridge and LAN Network adapters connection[7]

→ Power on the FortiGate and wait for it to finish the installation.

→ It will require a username and password. The username will be “admin” and the password will be blank.

→ For security reasons, the first thing you should do is change the default login credentials.

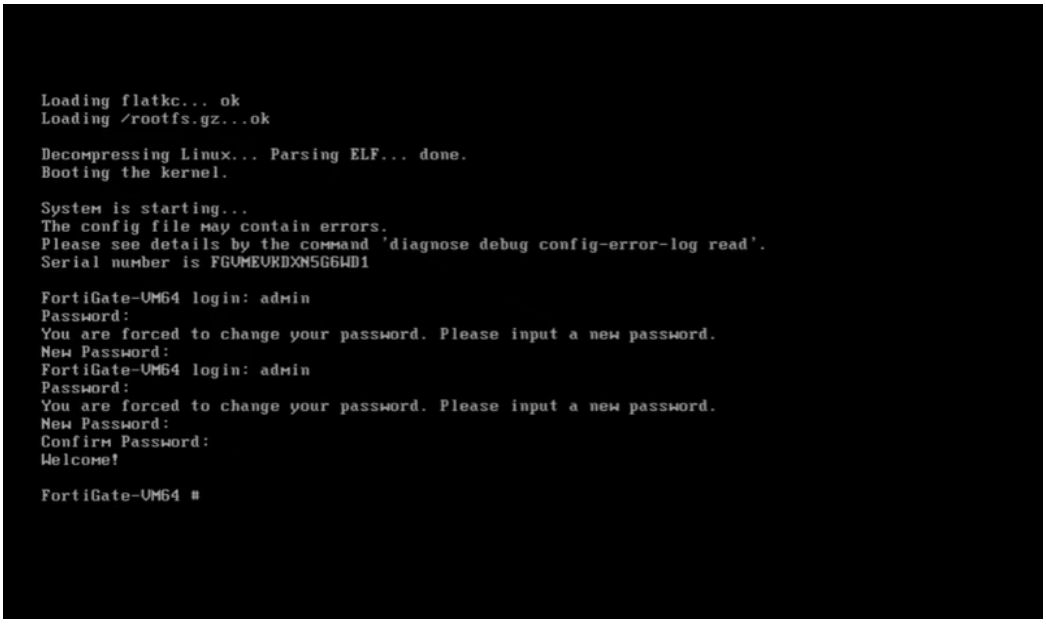


Figure 20: Power on FortiGate[7]

3.5 Configure FortiGate system interface

In FortiGate, various interface settings can be customized, such as aliases (identifiers for reference), IP addresses (public or private for connectivity), administrative access protocols (e.g., Https, ping, ssh), and DHCP servers (for dynamic IP assignment). You can choose between CLI or GUI for these configurations.

To set up your interfaces in GUI, follow these steps:

→ Assign IP Addresses: Configure IP addresses for internal and external interfaces based on your network design. Navigate to 'Network' → 'Interfaces' in the settings.

→ Define Roles: Specify roles for each interface (e.g., LAN, WAN).

For CLI access to the interface settings, use the appropriate commands.

→ Edit port1: This is the bridge network adapter which will be the Wan or the Internet interface.

→ Set mode DHCP

→ Set role WAN.

→ Set alias WAN.

→ Set allow access http https ssh telnet ping.

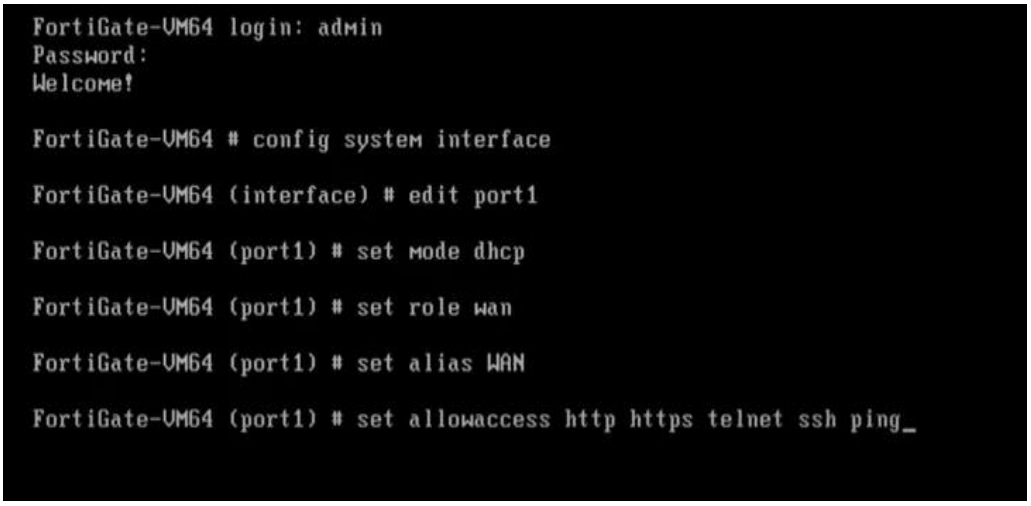


Figure 21: Port1 configuations[7]

Configure the LAN interface.

→ Next
→ Edit port2: This would be the LAN or the internal network.
→ Set mode static: since we are going to statically assign the IP address.
→ Set role LAN.
→ Set IP: your IP for your default gateway e.g.: 10.10.10.1/24 with slash 24 subnets.
→ Set allow access http https ssh telnet ping.
→ Set alias internal.
→ End.

Figure 22: Port2 configurations[7]

Get the IP address to access FortiGate GUI

→ **Get system interface physical**: This command will show you the IP address that was received from port1 or the bridge network adapter.

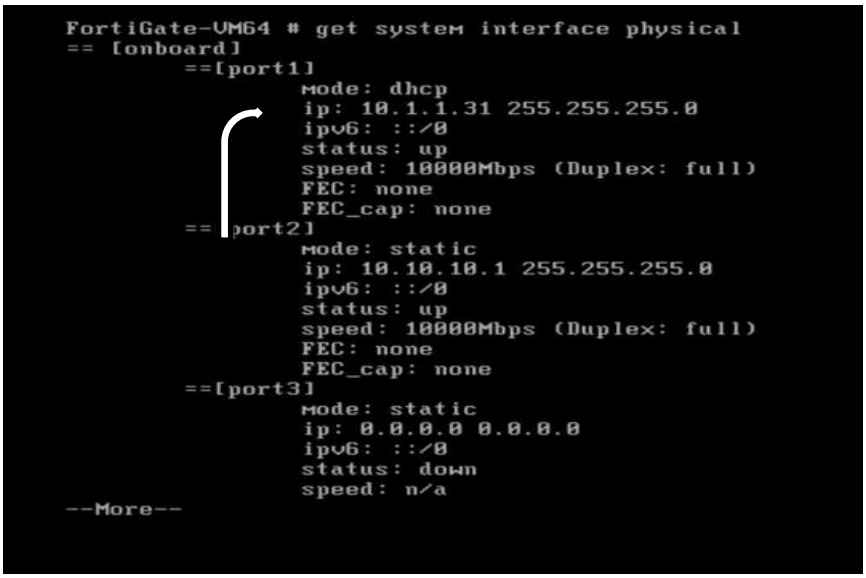


Figure 23:IP address to access the FortiGate interface[7]

→ To access the FortiGate GUI, copy the IP address you have and paste it into the browser.

→ Log in using the default username which is admin and the password admin as we configured.

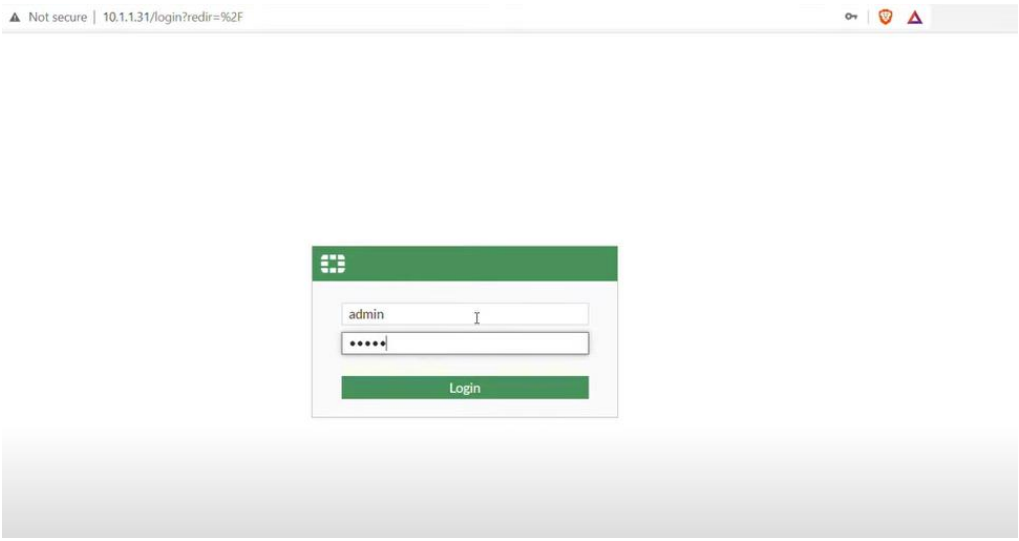


Figure 24: Log in to the FortiGate[7]

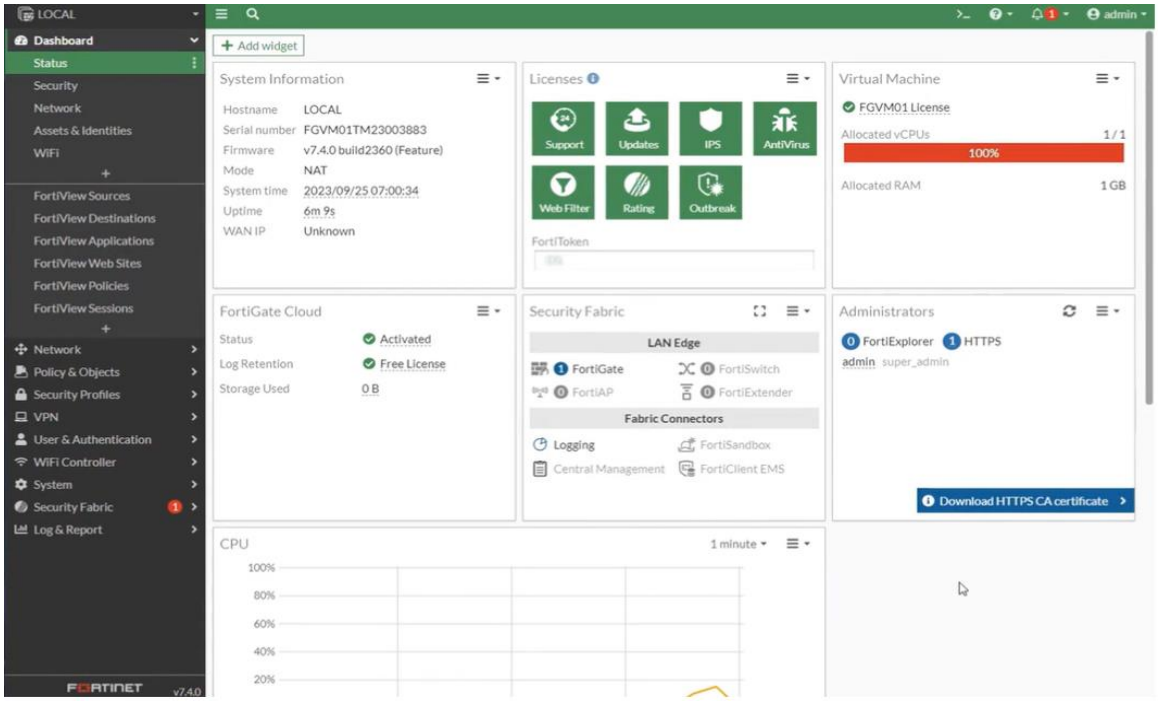


Figure 25: FortiGate GUI[7]

3.6 Configure Basic Network Settings

3.6.1 DHCP Server Configurations

A FortiGate interface can host a DHCP server that automatically assigns IP addresses to connected devices. You can establish multiple DHCP servers on any interface, customizing settings like IP address range allocation, subnet mask, default gateway (usually the interface IP), and DNS server (typically FortiGate's DNS server).

To configure the DHCP server for the internal network and enable automatic IP assignment to connected devices, follow these steps.

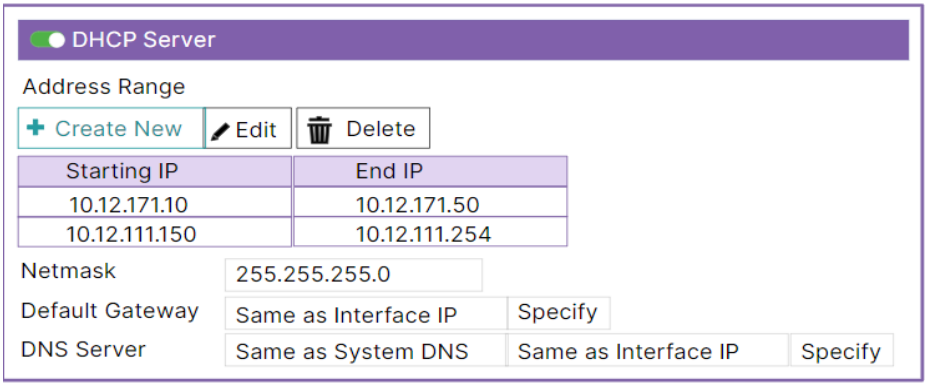


Figure 26: DHCP Server[7]

We can set up a DHCP server on port2 or port1 using GUI:

Go to Network > Interfaces > Enable DHCP >Port2/1, set the interface IP address as 192.168.1.1/24 and configure DHCP server on interface port2/1 (Range of IP addresses should be: 192.168.1.20 to 192.168.1.30, DNS: 4.2.2.4) and Enable Device Detection under Port2/1 to allows the FortiGate to identify and monitor devices connecting to this interface. This feature enhances network security and visibility.

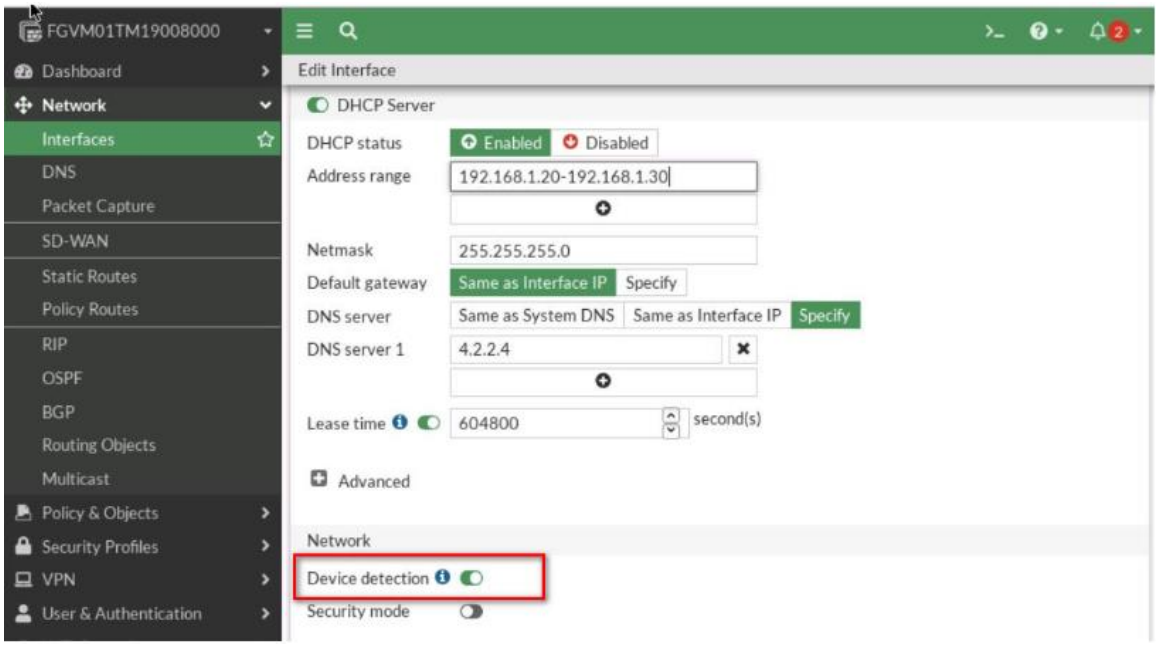


Figure 27: Enable DHCP server.[7]

3.6.2 Static routing

Static routing is a basic method used in network devices, including FortiGate firewalls. FortiGate typically has a default route for internet access, and in complex setups, static routes are used. These routes are stored in a routing table to guide incoming traffic.

The default route is like telling FortiGate, "If you're not sure where to send the traffic, send it here." It allows all devices connected to FortiGate to access the internet, using a general address (0.0.0.0) for any web destination.

This route directs traffic to another router, often through the WAN port, ensuring internal traffic can reach the internet. Proper routing is crucial for this.

Type	Destination	Gateway IP	Interfaces	Distance	Priority
Static	10.100.00/16	10.10.1.1	To-HQ-B	10	1
Static	10.101.00/16	10.0.10.1	To-HQ-A	10	1
Static	10.102.00/16	10.0.12.1	To-HQ-MPLS	10	5
Static	0.0.0.0/0	10.0.68.1	Internet_A	10	1

Figure 28: Static routing table. [7]

→ Set a Static route in the firewall to reach the NAT object. Go to Network > Static Route > Create a new. This way for optimizing network performance and enhancing control over data routing.

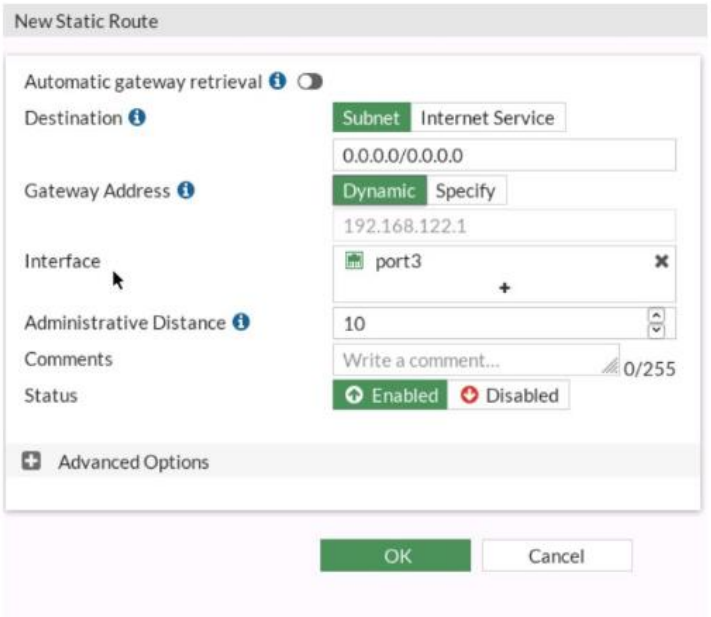


Figure 29: Configure a static Routing[7]

3.6.3 Create Policies

Creating policies is a fundamental aspect of managing and controlling various aspects of a system or network. In this context, this section explores how to create policies, specifically focusing on the Internet Access Control Policy. This policy empowers users to govern and permit specific types of traffic from their local network to the internet, offering essential control and security through firewall configurations.

→ Go to Policy & Objects > Firewall Policy section, click Create New to add a new firewall policy, and configure the following settings:

Name: LocalToInternet

From inside to outside (port2 to port3)(LAN to WAN)

Source: Create an address for local network (Subnet: 192.168.1.0/24)

Destination: all

Schedule: Always

Service: Only HTTP, HTTPS, DNS, Ping

Action: Accept

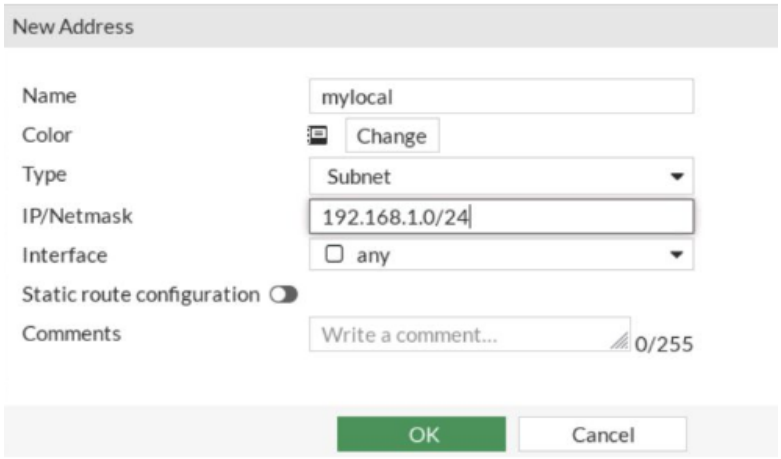


Figure 30: Set local subnet[7]

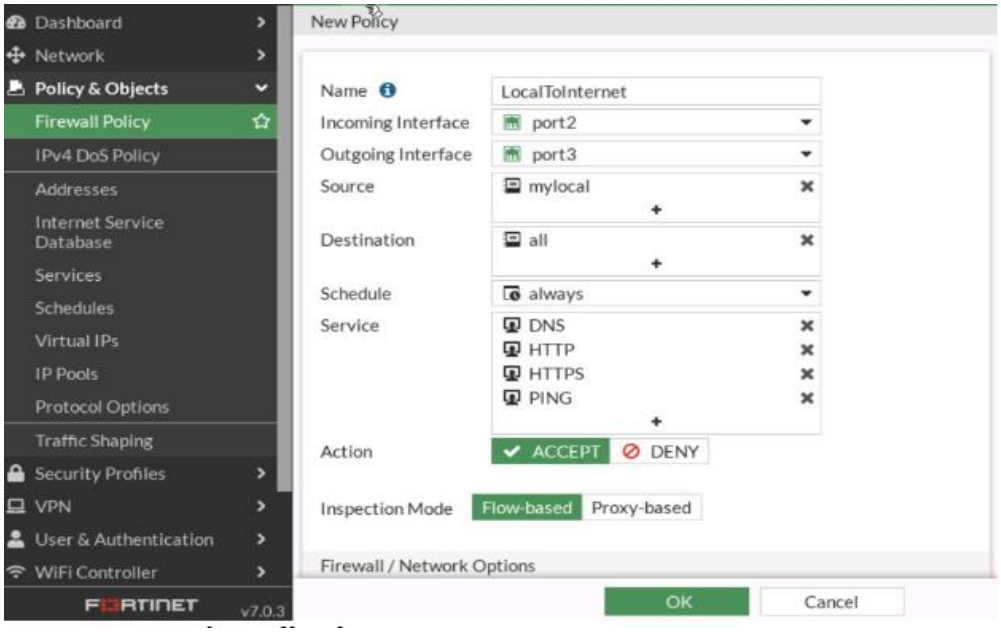


Figure 31: Set Firewall Policy[7]

3.6.4 Configuring SD-WAN

SD-WAN enhances network performance by optimizing WAN and multi-cloud connectivity. It dynamically selects paths like MPLS, 4G/5G, or broadband for efficient access to cloud apps. FortiGate firewall configuration for SD-WAN improves routing, increasing bandwidth usage, network resilience, and overall performance.

Here are the steps for FortiGate SD-WAN policy setup.

→ Create or Identify WAN Interfaces

→ Go to Firewall > Network > Interfaces > port4. Set Name as WAN2 and IPv4 as 10.200.2.1/24(e.g.). Ensure you have at least two WAN interfaces configured (e.g. WAN1 and WAN2). These interfaces will be used for SD-WAN, do the same configurations for both WAN1 and WAN2.

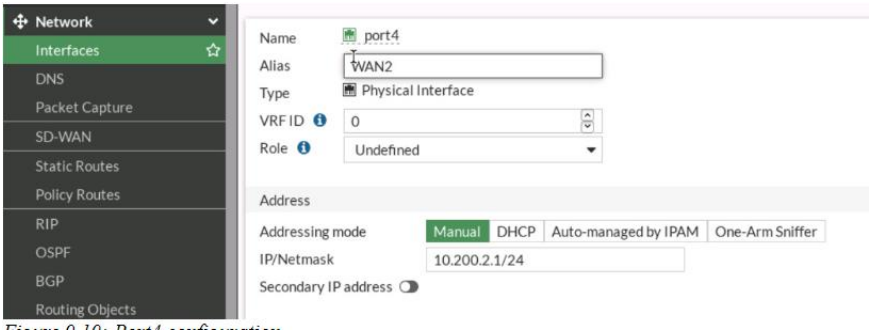


Figure 32: Port4 configuration[7]

→ Configure SD-WAN Members.

→ Navigate to Network > SD-WAN > SD-WAN Interfaces.

→ Click on Create New to add your WAN interfaces to the SD-WAN interface.

→ Select the WAN interfaces (WAN1, WAN2, etc.) you wish to include in your SD-WAN setup. Configure the necessary settings for each interface, such as Cost, Weight, Priority, etc., based on your requirements.

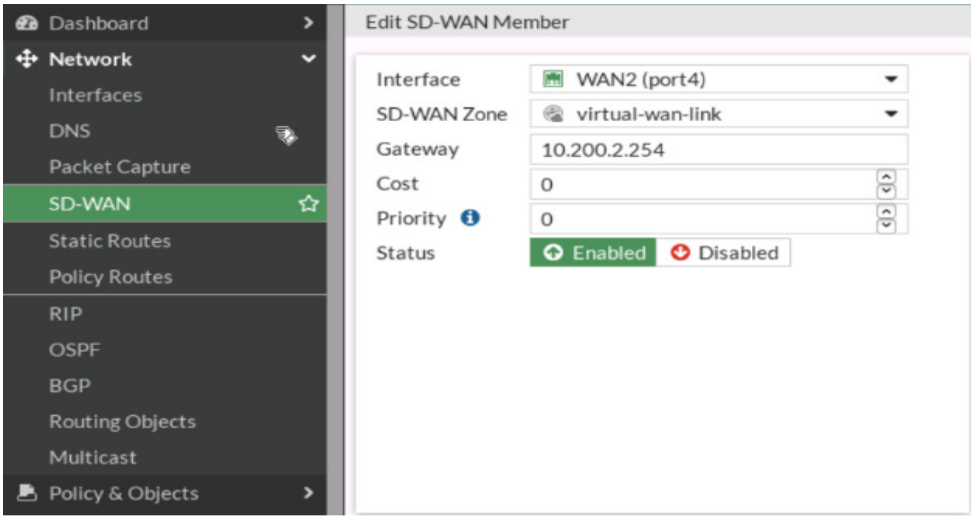


Figure 33: Add Port4 as SD-WAN members[7]

3.6.5 SD-WAN zones

SD-WAN zones in FortiGate are logical groups of WAN interfaces where you define policies for managing and optimizing traffic. You can see the SD-WAN zones from network > SD-WAN.

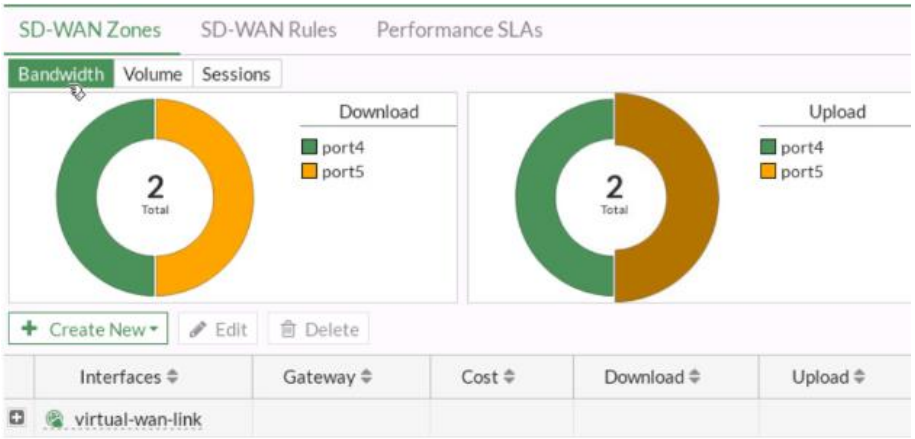


Figure 34: SD-WAN Zones[7]

3.7 IPv4 Policies

IPv4 policies are used to control traffic flow through the FortiGate unit. used to manage and control how IPv4 addresses are allocated and used across networks. These policies ensure the efficient and organized distribution of the limited IPv4 address space, facilitate routing and network management, and support security measures to protect network integrity.

→ Go to Policy & Objects > IPv4 Policy.

→ Create a New Policy by clicking on the "Create New" button.

→ Set Incoming and Outgoing Interfaces based on your network topology.

→ Configure Source and Destination Addresses; you can use predefined addresses or create new ones.

→ Set Service to specify which types of traffic are allowed through.

→ Action: Choose "Accept" to allow traffic or "Deny" to block.

→ Enable NAT if needed and configure any additional settings like security profiles.

→ Save the policy.

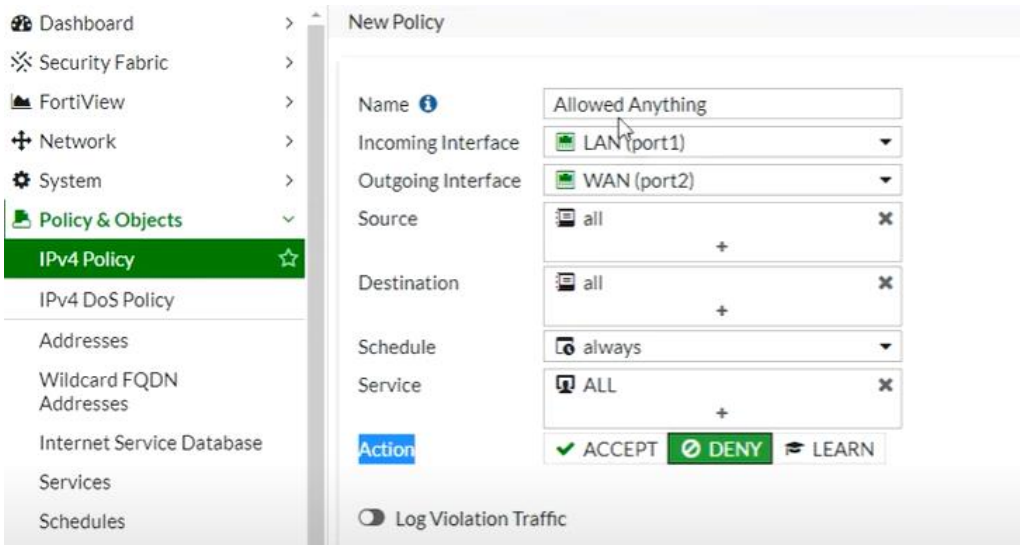


Figure 35: Create IPV4 Policy[7]

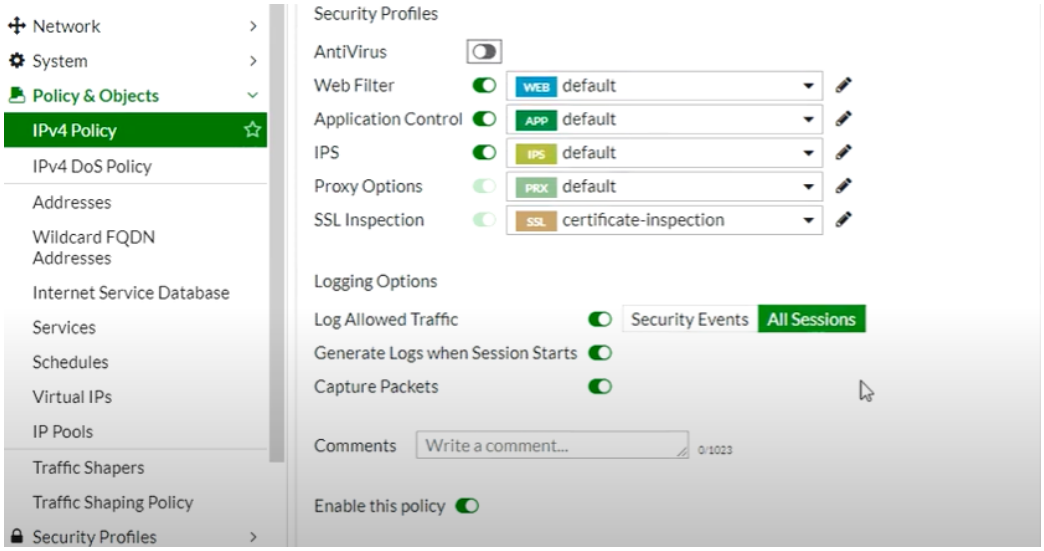


Figure 36: IPV4 Security profiles[7]

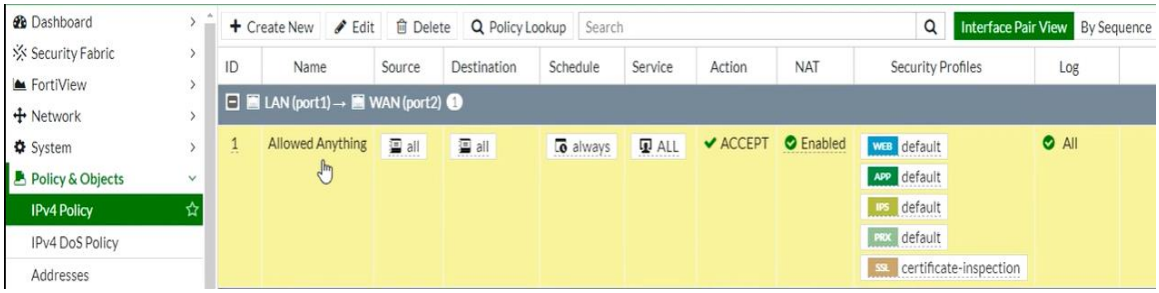


Figure 37: IPV4 Allow anything policy

3.7.1 IPv4 Denial of Service (DoS) Policies

IPv4 Denial of Service (DoS) policies are measures to protect networks from DoS attacks, which aim to protect the network from potential DoS attacks by monitoring, logging, and blocking malicious traffic based on anomalies detected at both the Network and Transport layers of the OSI model.

- → Go to Policy & Object > IPV4 DOS Policy:
- → Name: DOS
- → Incoming Interface: Port1
- → Source, Destination, Service: all
- → L3 Anomalies: Status and Logging: Enable, Action Block
- → L4 Anomalies: Status and Logging: Enable, Action Block

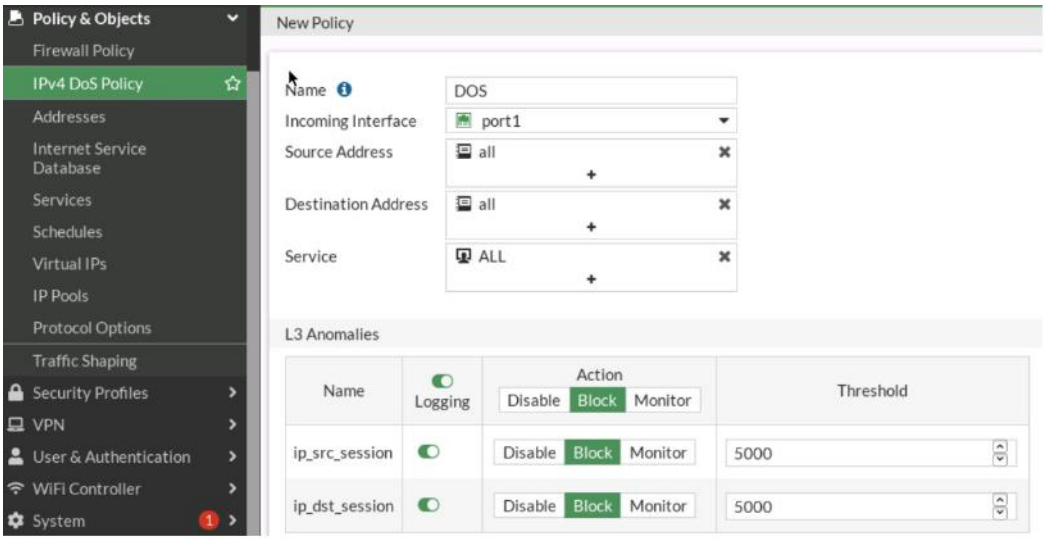


Figure 38: IPV4 DOS policy[7]

If you have a network topology you can do this scenario to check the policy.

Scenario: set a DDoS Prevention on traffic from Port1 to Port2. and install a script in kali to do a DOS attack .and set a DDoS Prevention Policy to block DOS traffic in FortiGate to see the report of the attack go to:

→ Log & Report **>** Anomaly**.**

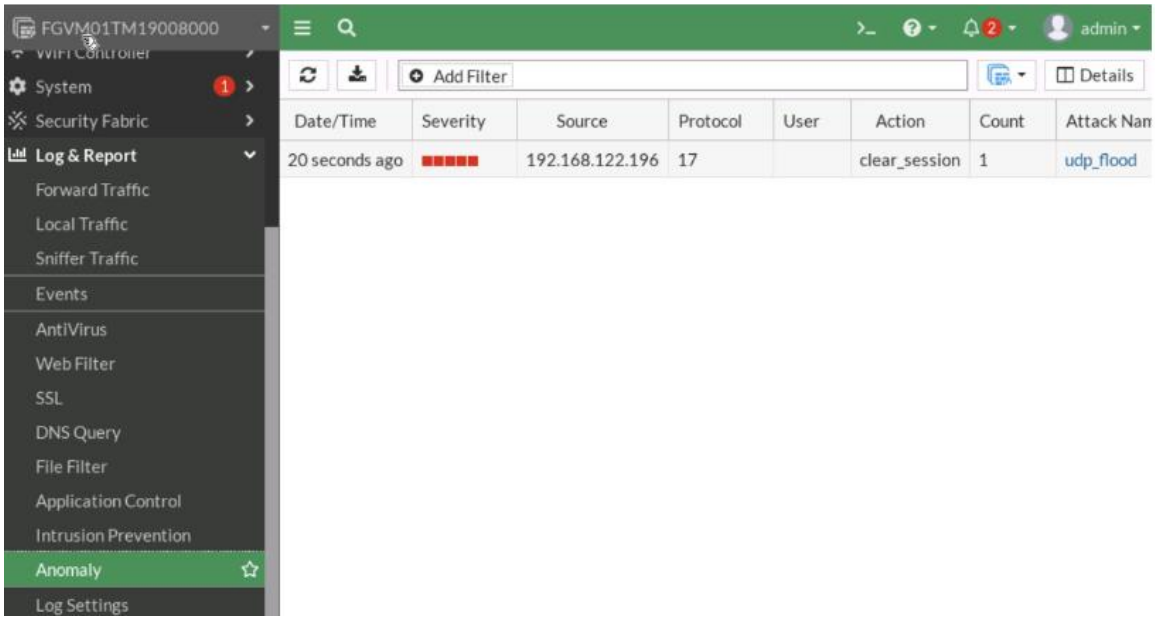


Figure 39: View anomaly report

→ Go to Dashboard > Security > Top Threats and verify your result.

this section displays the most significant security threats currently detected by the FortiGate unit.

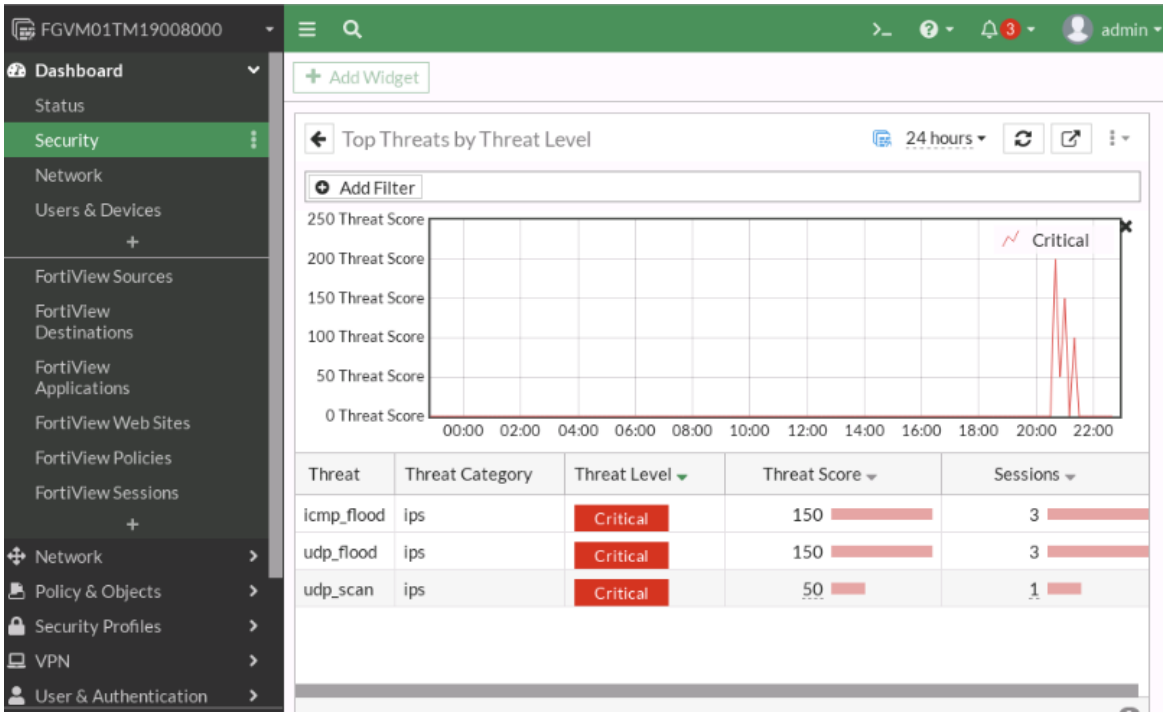


Figure 40: Security threats currently detected[7]

3.8 Site-to-Site VPN Configurations

A Site-to-Site VPN configuration securely connects multiple networks across different locations, allowing them to share data over the internet as if they were on the same private network securely.

→ Go to VPN > IPsec Wizard.
→ Choose a Template Type: Select "Site to Site" and provide a descriptive name.
→ Set the Remote Gateway to the public IP address of the other VPN endpoint.
→ Configure Authentication by setting a pre-shared key.
→ Set Local and Remote LANs to define which networks will be accessible through the VPN.
→ Review the settings and complete the wizard.

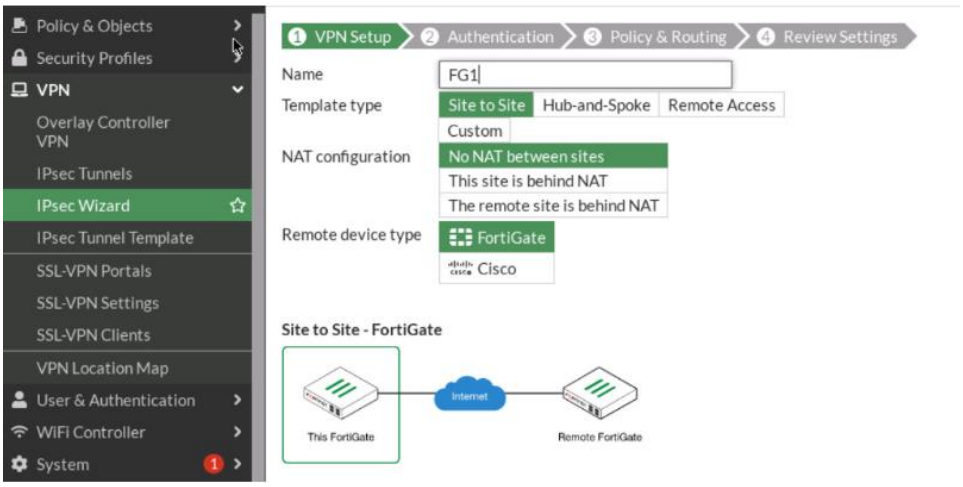


Figure 41: VPN setup[7]

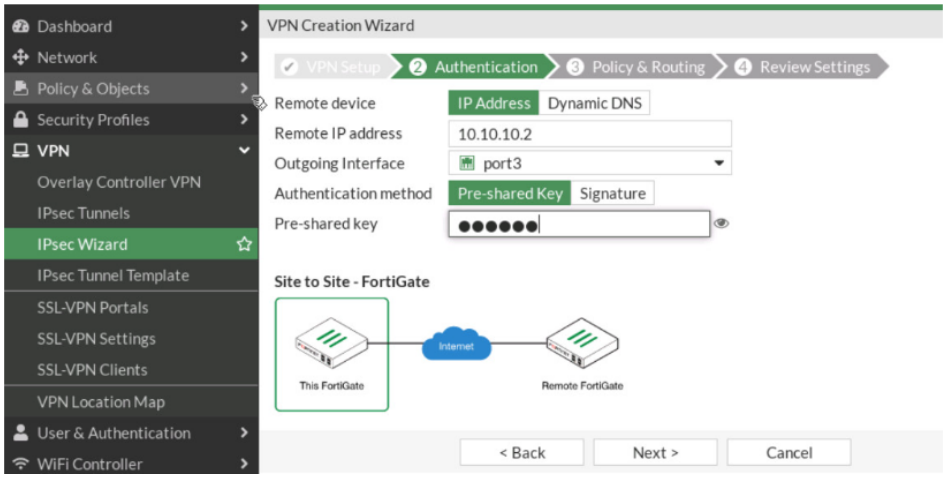


Figure 42: Authentication[7]

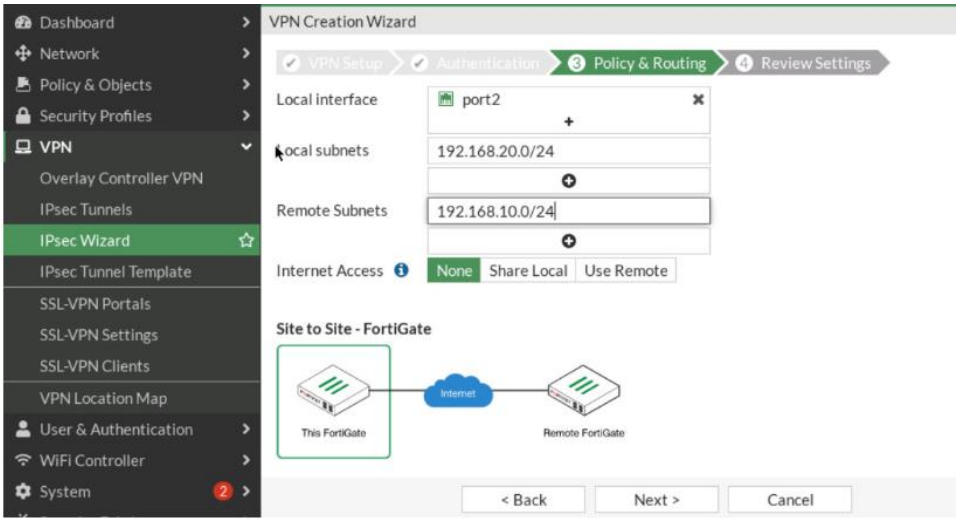


Figure 43: Policy & Routing[7]

→ Then configure the FG2 in the same way.

→ Go to your IPsec Tunnels and double click on Inactive to troubleshoot or activate the VPN tunnel you've just set up.

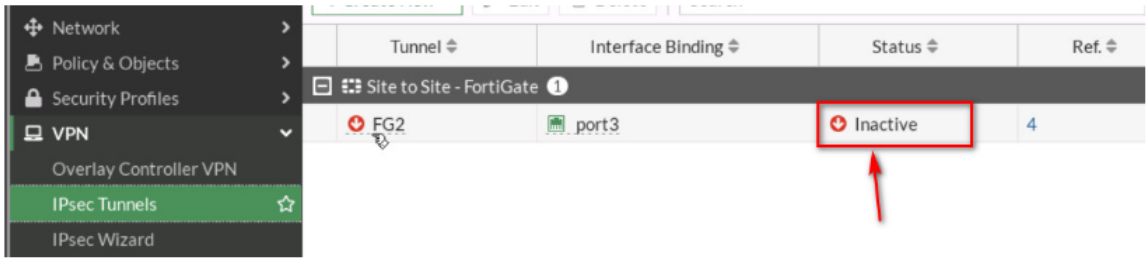
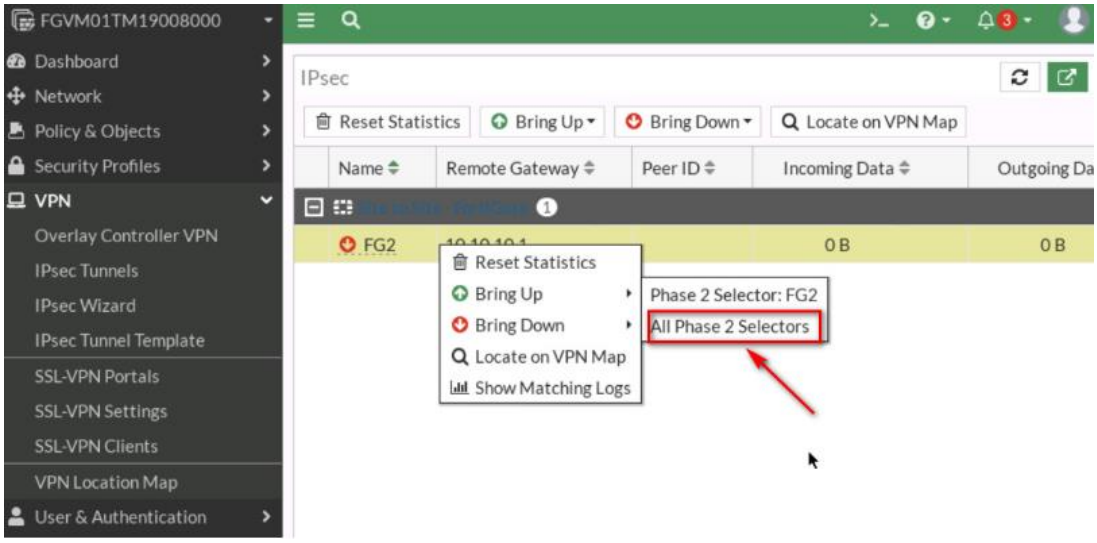


Figure 44: Configure IPsec Tunnels[7]

→ On the next windows, right click on the tunnel > Bring UP > All Phase 2 selectors. Then, your tunnel should be up!



Bring up IPsec Tunnel

This step is manually for initiating a VPN tunnel in network devices like FortiGate. Secure communication between VPN endpoints is started by activating all configured traffic routes within the tunnel. This action is necessary for ensuring the VPN tunnel is operational, allowing for encrypted data exchange according to the VPN's setup. It's commonly used for testing, troubleshooting, or activating the tunnel after configuration changes.[8]

[8] Hauser et al., "P4-IPsec: Site-to-Site and Host-to-Site VPN in P4-Based SDN," IEEE Access, Volume 8, July 2020

3.8.1 Virtual IP (VIP) NAT Configuration

Virtual IPs are used for forwarding traffic from external IP addresses to internal IPs and ports.

→ Go to Policy & Objects > Virtual IPs.

→ Create a New VIP by clicking on "Create New".

→ Set External and Mapped IP Addresses; the external IP is the one the public uses to access the internal resource.

→ Configure Port Forwarding if specific services need to be accessible externally.

→ Use the VIP in an IPv4 Policy to allow traffic to the internal resource.

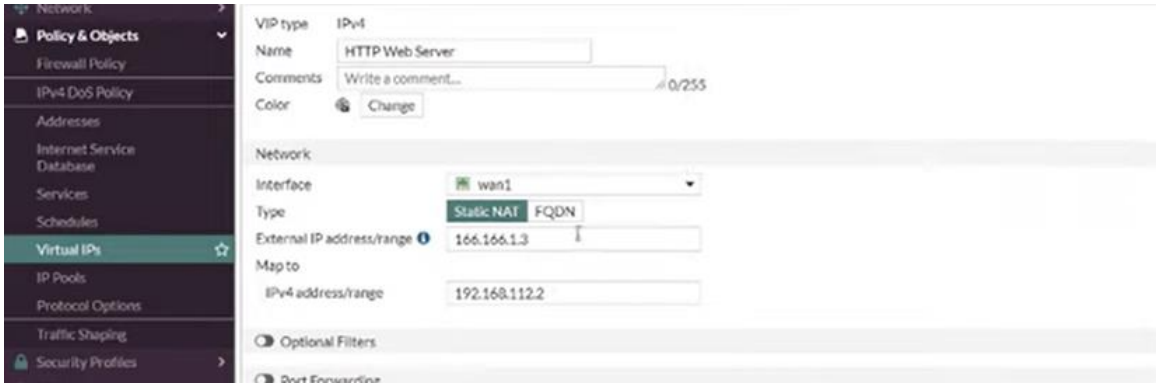


Figure 45: VIP configurations[7]

3.9 High Availability

Configuring High Availability (HA) on FortiGate devices, involving one primary (active) and at least one secondary (passive) firewall, ensures network continuity by providing redundancy and increasing reliability. This setup allows for a seamless transition to the secondary unit, which becomes the primary if the active firewall is disabled, thereby maintaining operational integrity even in the event of a unit failure.

1. Preparing for HA Configuration

→ Compatibility Check: Ensure all FortiGate units are of the same model and are running identical FortiOS versions.

→ Backup Configurations: Before proceeding, back up the current configuration of all units involved in the HA setup.

2. Configuring the HA Settings

→ Go to System > HA in the FG-Primary:

→ Initiate HA Setup: Click on "Change" to enable HA configuration options if they are not already available.

→ Select the Mode: Active-Passive

→ Device Priority: 128 (The higher priority is primary)

→ Group Name: HRT (Assign a name for the HA cluster, the Group name between Primary and Secondary should be the same)

→ Password: Set a password (The Password between Primary and Secondary should be the same)

→ Monitor Interface: Port 3

→ Heartbeat Interface: Port 4

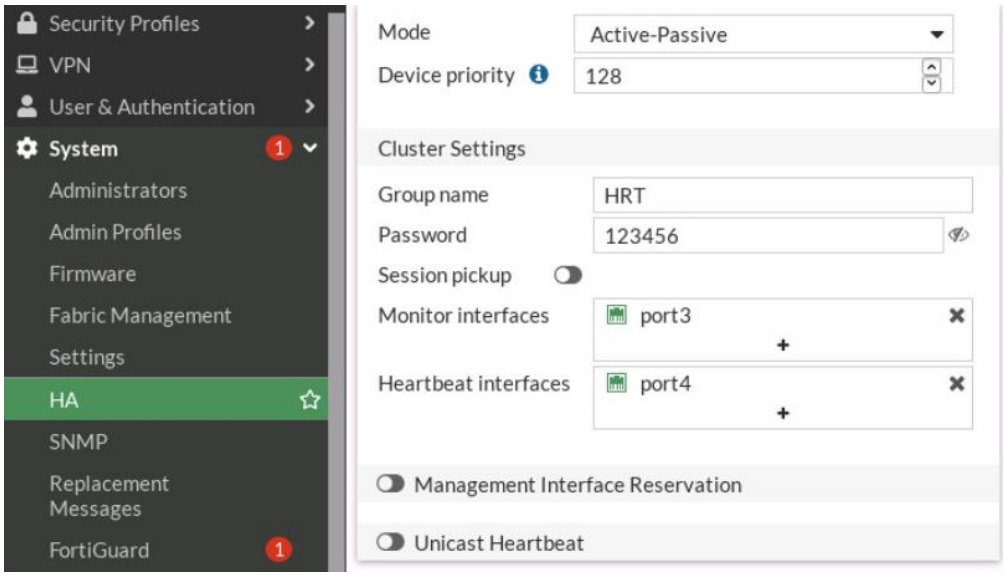


Figure 46: HA primary configuration [7]

→ Do the same configuration in the FG-Secondary but set the Device priority to 50.

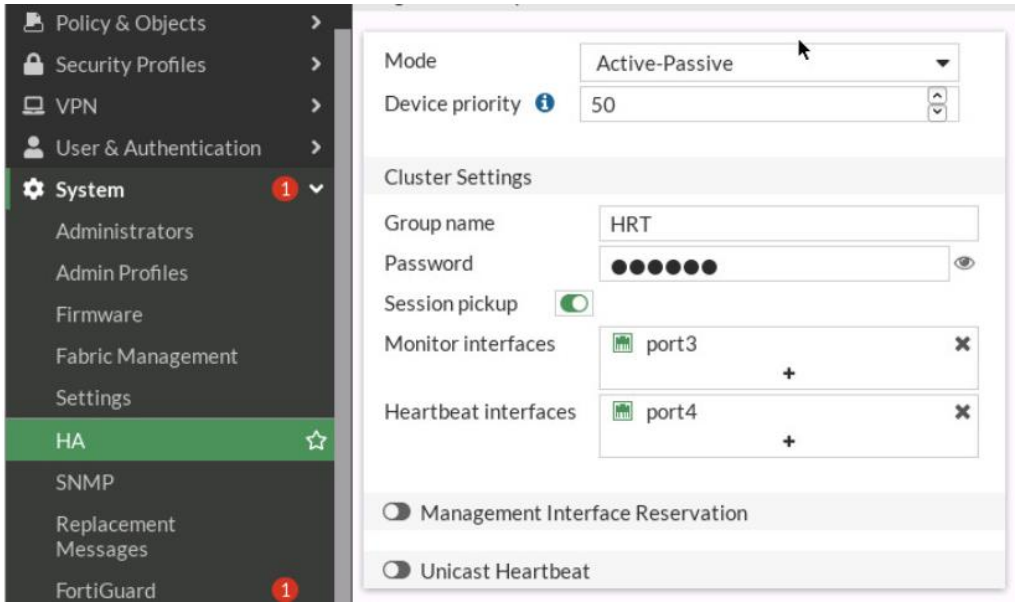


Figure 47: HA secondary configuration[7]

After setting secondary device, no longer be able to access secondary device because In an HA configuration, the primary device takes an active role, handling the traffic and management tasks, while the secondary device remains in standby mode, ready to take over if the primary device fails or becomes unavailable.[8]

→ Go to FG-Primary **>** System **>** HA and evaluate your result.

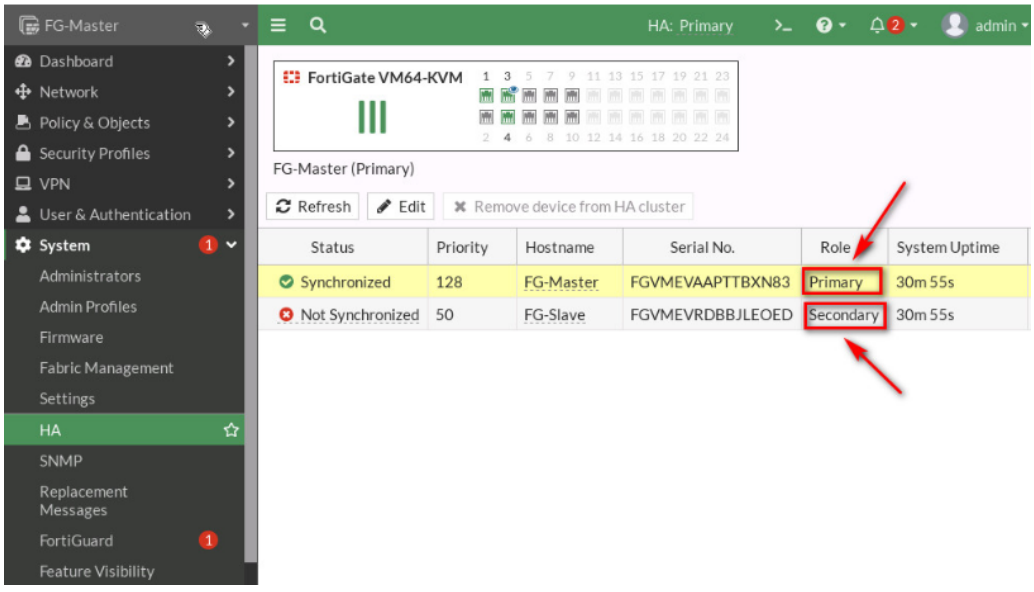


Figure 48: HA Status [7]

→ The two devices will be synchronized after a while.

Status	Priority	Hostname	Serial No.	Role	System Uptime
Synchronized	128	FG-Master	FGVMEVAAPTTBXN83	Primary	36m 7s
Synchronized	50	FG-Slave	FGVMEVRDBBJLEOED	Secondary	36m 7s

Figure 49: HA Synchronized status[7]

Figure 50: Verify firewall role after stopping FG-Primary[7]

To verify your result:

→ Go to Log & Report > Events > HA Events and download the log.

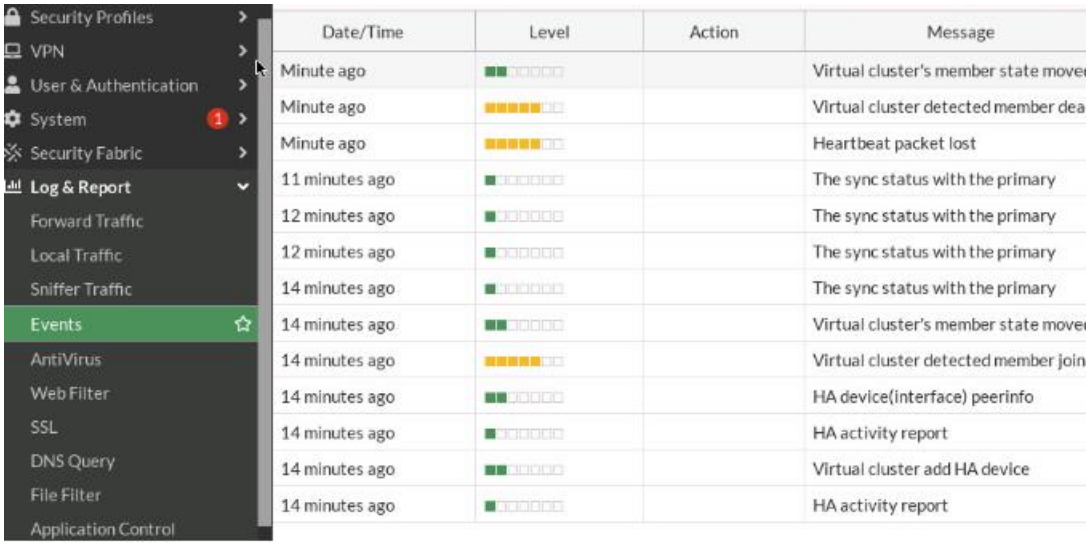


Figure 51: HA Events[7]

4 Regular Maintenance, Support and Training

4.1 Regular Maintenance

It is important to perform regular maintenance, use support resources, and engage in continuous training to keep the FortiGate firewall working well. This section explains how to keep the FortiGate firewall working well, troubleshoot common issues, get help, and keep up with training resources.

4.1.1 Firmware Updates

- **Importance:** Keeping the firewall firmware up-to- security fixes for vulnerabilities, improvements in performance, and new features.
- **Instructions:**
-

Option 1: Upgrade from Fortinet Support Portal

1. **Check for Updates**: Log in to the Fortinet support portal at support.fortinet.com.
2. **Download the Latest Firmware:** Navigate to the firmware download section and download the appropriate firmware for your FortiGate model.
3. **Backup Configuration:** Before updating, backup the current configuration by navigating to System > Maintenance > Backup & Restore.
4. **Upload and Install Firmware:** Follow the portal instructions to upload and install the new firmware on your FortiGate device.
5. **Verify Operation:** After the update, verify that the firewall is operating correctly and that all configurations are intact.

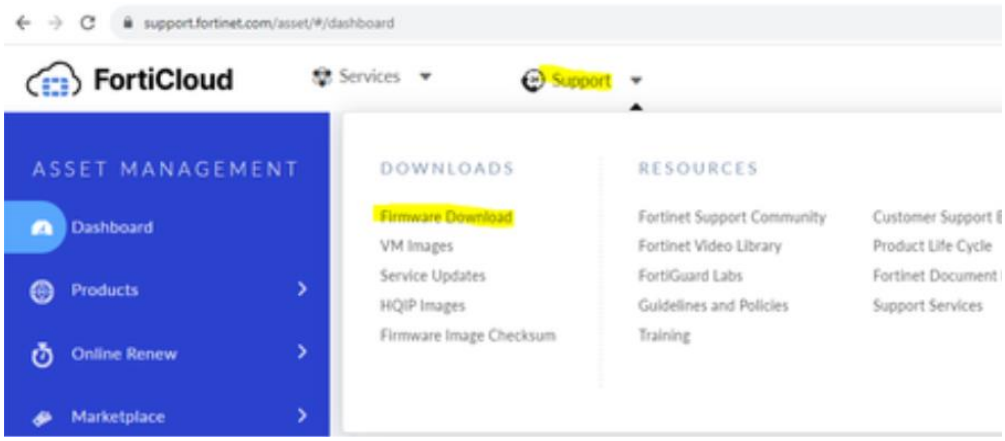


Figure 52: Upgrade from Fortinet Support Portal Part 1

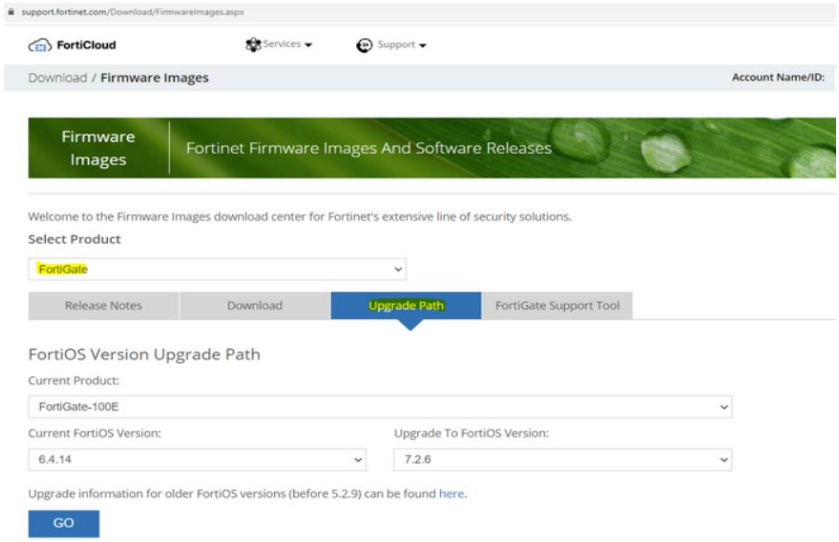


Figure 53: Upgrade from Fortinet Support Portal Part 2

Option 2: Upgrade from the GUI:

1. **Log in to the FortiGate GUI:** Open a web browser and enter the IP address of your FortiGate device to access the GUI as the administrative user.
2. Go to **Dashboard -> System Information**.
3. **Check for Updates:** Click on "Check for updates" to see if a new firmware version is available.
4. Select '**Update'** next to **'Firmware Version,'** then select Browse and find the previously downloaded firmware image file.
5. **Backup Configuration:** Before updating, backup the current configuration by clicking on Backup.
6. **Reboot:** Allow the device to reboot to complete the firmware update.
7. **Verify Operation:** After the update, verify that the firewall is operating correctly and that all configurations are intact.

Figure 54: Upgrade from the GUI – Part 1

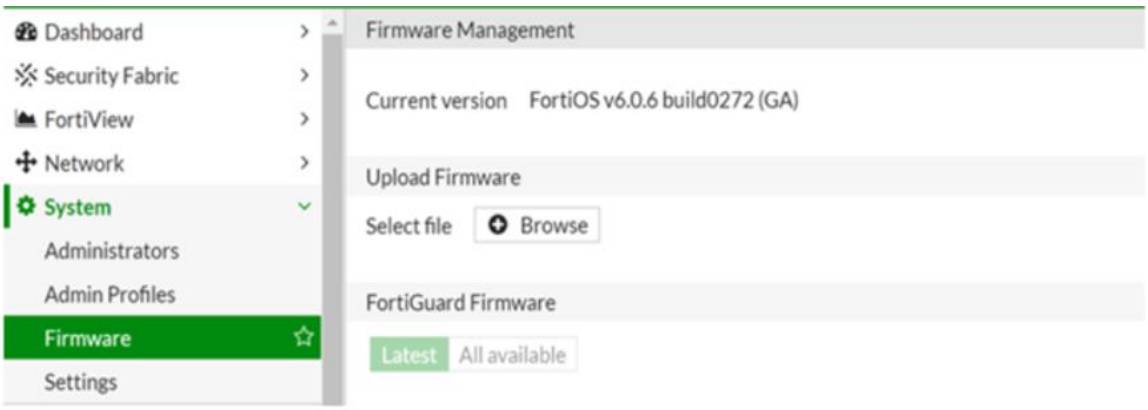


Figure 55:Upgrade from the GUI Part 2

4.1.2 Configuration Backups

- **Importance**: Regularly backing up the firewall configuration ensures that you can quickly restore the system in case of a failure or misconfiguration.
- **Instructions:**
  1. **Scheduled Backups**: Set up automated backups by navigating to System > Maintenance > Backup & Restore.
  2. **Manual Backups:** Perform manual backups periodically or before making significant changes to the configuration.

4.1.3 Performance Monitoring

- **Importance**: Monitoring the performance of the firewall helps identify and address potential issues before they impact network operations.
- **Instructions**
  1. **Monitor Logs:** Regularly check the firewall logs for unusual activity by navigating to Log & Report > Log Settings.
  2. **Analyze Traffic**: Use the traffic monitoring tools in the FortiGate interface to analyze network traffic patterns and identify any performance bottlenecks.

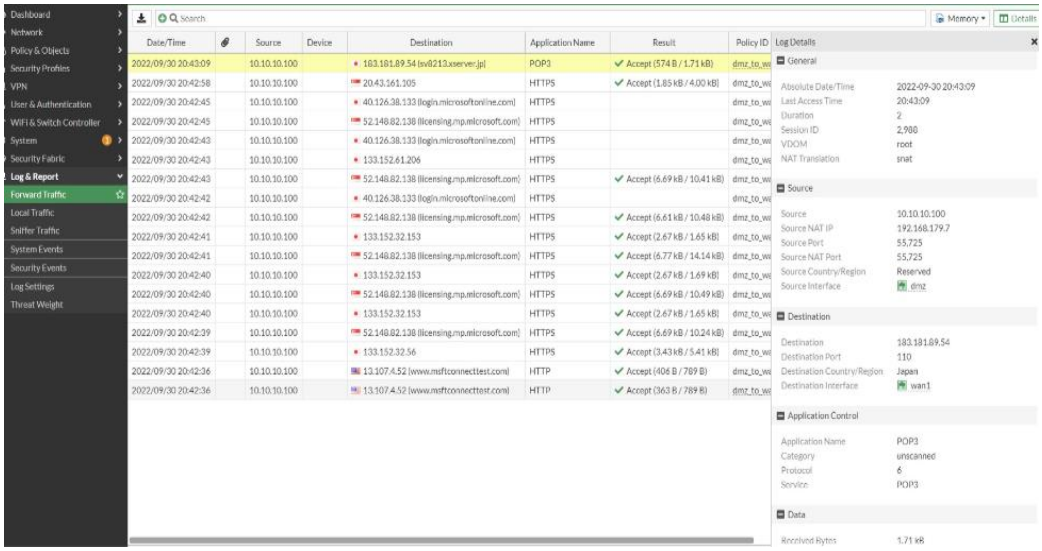


Figure 56: Performance Monitoring

4.2 Troubleshooting

4.2.1 Common Issues and Resolutions

- **Connectivity Problems:** Check the network cables, check the interface configuration, and make sure that the correct IP addresses are assigned.
- **Policy Issues:** Check firewall policies to make sure they are set up correctly and that no rules are blocking traffic that is needed.
- **Performance Changes:** Check for high CPU or memory usage and optimize configurations to reduce load. Consider upgrading hardware if necessary.

4.2.2 Diagnostic Tools

- **Ping and Traceroute:** Use these tools to diagnose network connectivity issues.
- **Packet Capture:** Capture and analyze packets to troubleshoot complex network problems.

To use the packet capture tool in the GUI:

1. Go to Network > Diagnostics and select the Packet Capture tab.

2. Optionally, select an Interface (any is the default).

3. if needed, enable Filters and select a Filtering syntax:

a) **Basic:** enter criteria for the Host, Port, and Protocol number.

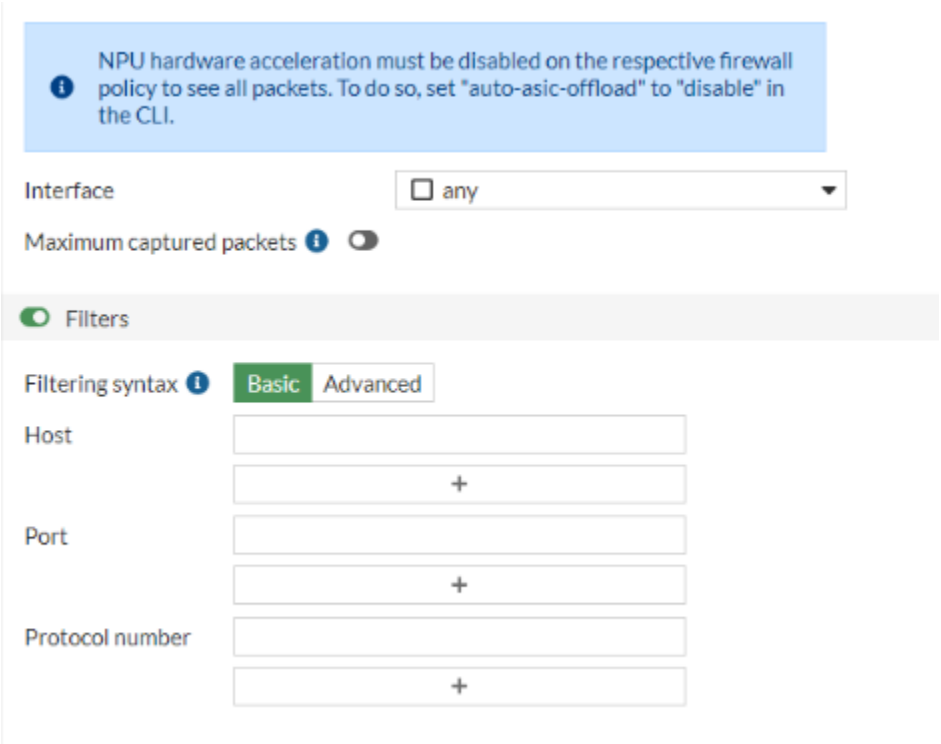


Figure 57: Packet Capture – basic

b) **Advanced:** enter a string, such as src host 172.16.200.254 and dst host 172.16.200.1 and dst port 443.

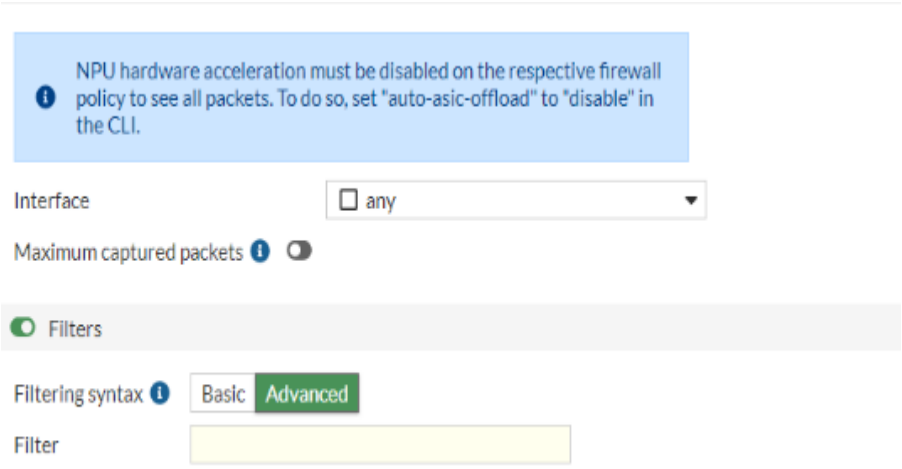


Figure 58: Packet Capture – advanced

4. Click Start capture.

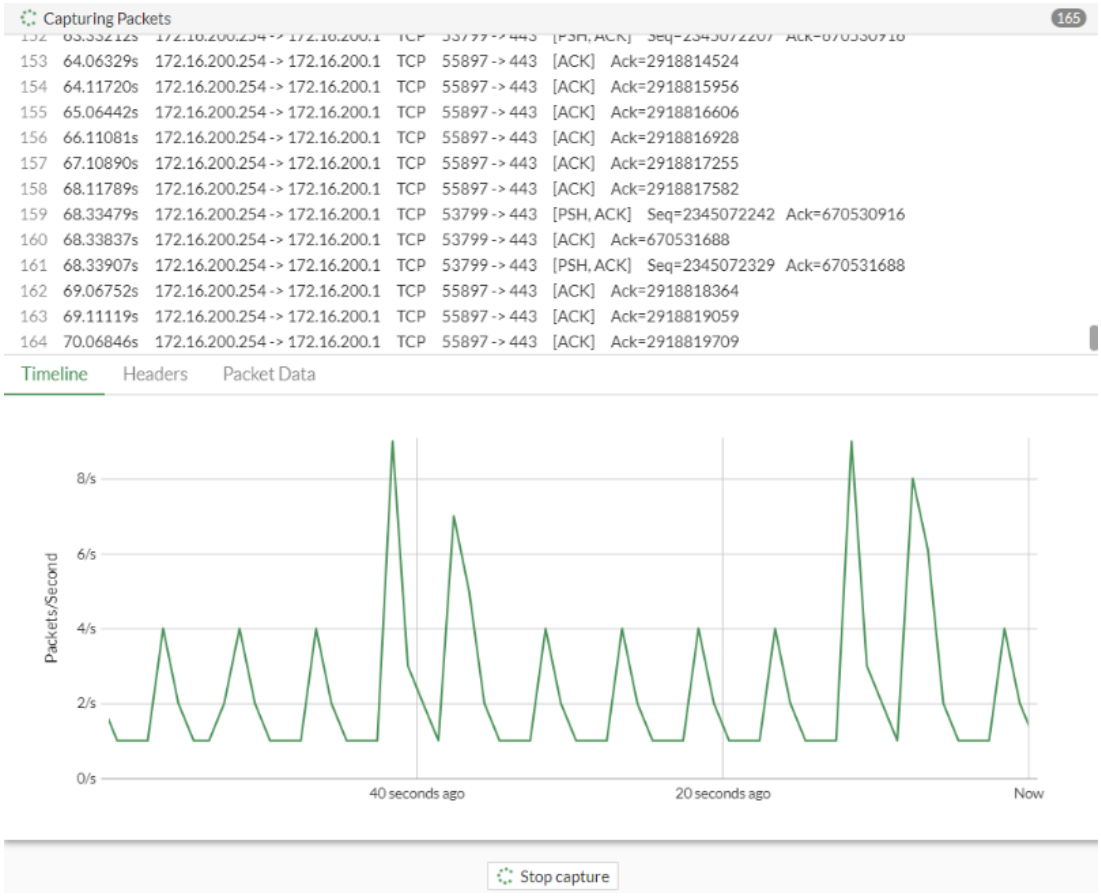


Figure 59: Packet Capture – click start

- **Log Analysis:** Utilize FortiGate's log analysis tools to identify and resolve issues by navigating to Log & Report > Log Settings.

4.3 Support Resources

4.3.1 Fortinet Support

- **Support Portal:** Access the Fortinet support portal at support.fortinet.com for technical assistance, documentation, and firmware updates.
- **Support Contracts:** Ensure that your FortiGate device has an active support contract to access technical support and advanced replacement services.
- **Community Forums:** Participate in the Fortinet community forums to seek advice and share knowledge with other FortiGate users.

4.3.2 Documentation and Manuals

- **Official Documentation**: Refer to the official Fortinet documentation for detailed information on configuring and managing FortiGate firewalls. Access it at docs.fortinet.com.
- **User Manuals**: Keep the FortiGate user manuals handy for reference during configuration and troubleshooting.

4.4 Training and Additional Resources

4.4.1 Fortinet Training and Certification

- **Courses:** Enroll in Fortinet's training courses, such as the Network Security Expert (NSE) program, to deepen your knowledge of FortiGate firewalls and network security.
- **Certification:** Obtain Fortinet certifications to validate your expertise and improve your ability to manage and maintain FortiGate devices effectively.

4.4.2 Interactive Learning

- **Video Tutorials:** Utilize video tutorials and webinars available on the Fortinet website and YouTube channel for visual learning and step-by-step guidance.
- **Simulations:** Engage in hands-on simulations and lab exercises to practice configuring and managing FortiGate firewalls in a controlled environment.

5 References

Azzam, Ahmad; Munadi, Rendy, Mayasari, Ratna (2019). Performance Analysis Of Firewall As Virtualized Network Function On VMware ESXi Hypervisor: JURNAL INFOTEL 11(1):29

Fattahillah, Novandi Rizki Nurfadila, Farah; Setiawan, Yanto (2023): High Availability's Implementation on the FortiGate Firewall Using SD-WAN Zone and HA Cluster: Active Vol. 2 No. 11 (2023): Indonesian Journal of Multidisciplinary Science

Fortinet Community https://community.fortinet.com/t5/FortiGate/Technical-Tip-DoS-attack-log-according-to-action-set-on-DoS/ta-p/198465 [Accessed January 18, 2024].

Fortinet Product Infos https://www.fortinet.com/ [Accessed January 25, 2024]

Hauser et al., "P4-IPsec: Site-to-Site and Host-to-Site VPN in P4-Based SDN," IEEE Access, - Volume 8, July 2020

Liang, J. / Kim, Y. (2022). Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall, IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)

Palestine Money Authority, https://www.pma.ps/en/ [Accessed January 17, 2024].

Palo Alto, The Evolution of Firewalls, https://www.paloaltonetworks.com/resources/infographics/the-evolution-of-firewalls [Accessed January 18, 2024]

Schneider, B. (2000). Secrets & Lies, John Wiley & Sons.

Wack, J., Cutler, K. and Pole, J. (2002), Guidelines on Firewalls and Firewall Policy, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD [Accessed January 25, 2024]