

## **Introduction**

This write up features 2 labs, one consists of setting up a brand new FortiGate 40F firewall, setting up a user ID and updating to 6.4.14. The Second lab required us to upgrade FortiGate 40F from 6.4.14 to a version of 7.x. This is done for security reasons as support for 6.4 ends on September 30, 2024. We had to decide between 7.0, 7.2, and 7.4, all of which have their pros and cons such as security, maturity and feature set.

## **Background Information**

The FortiGate 40F is a “next-gen” firewall that enables small and midsize businesses (SMB) to get enterprise level security on a budget. Featuring many integrated security services such as: Firewall, VPN, Antivirus, Intrusion prevention, Web Filtering and application control, safeguarding your network from threats and provide control of network traffic.

Setting up your FortiGate 40F is very simple consisting of five simple steps such as setting up a Hostname, Registering for FortiCare, setting up a secure password, and setting up your Dashboard and upgrading the Firmware. The FortiGate 40F will come with 6.4.6 preinstalled which will require you to at least upgrade to 6.4.14. However, it is not recommended to stay on this version as end of life will arrive in just a few months on September 30<sup>th</sup>, 2024.

There are 2 types of support for a FortiGate firewall consisting of “End of Engineering support” which is the day Fortinet will stop providing non-critical updates to the OS version (usually 36 months after initial release). These include new feature sets and quality of life changes but there will be still updates that patch security vulnerabilities and critical issues/bugs. “End of Support” is often called End of Life as Fortinet will no longer give any updates to the OS version even if there is a major security issue found on that version. Someone should always update their Firewall before this day to keep their firewall’s security up to date and not expose yourself to security vulnerabilities.

Upgrading past 6.4.14 will have one deciding what is best to use, 7.0, 7.2, or 7.4. All of these FortiOS versions have their pros and cons based off the feature

set, OS maturity, time till End of (Engineering) Support and time till End of Life.

7.0 is the most mature coming out nearly 3 years ago on March 30<sup>th</sup>, 2021, however this version will reach its engineering support on March 30<sup>th</sup>, 2024. End of Life for 7.0 is September 30<sup>th</sup>, 2025. This is the version the Fortinet Community forum recommends for the FortiGate 40F.

7.2 is still considered mature and a stable version of FortiOS. Released nearly 2 years ago on March 31<sup>st</sup>, 2022, this version has more features than 7.0 while still providing stability. Engineering support will end on March 31<sup>st</sup>, 2025, and End of Life on September 30<sup>th</sup> 2026.

7.4 is considered brand new and still yet to mature. Coming out less than a year ago on May 11<sup>th</sup>, 2025, it is the newest version of FortiOS with the largest feature set. It is however due to it lacking maturity there may still be bugs and possible security vulnerabilities. End of Engineering support will end on May 11 2026 while End of Life on November 11 2027.

## **Lab Summary**

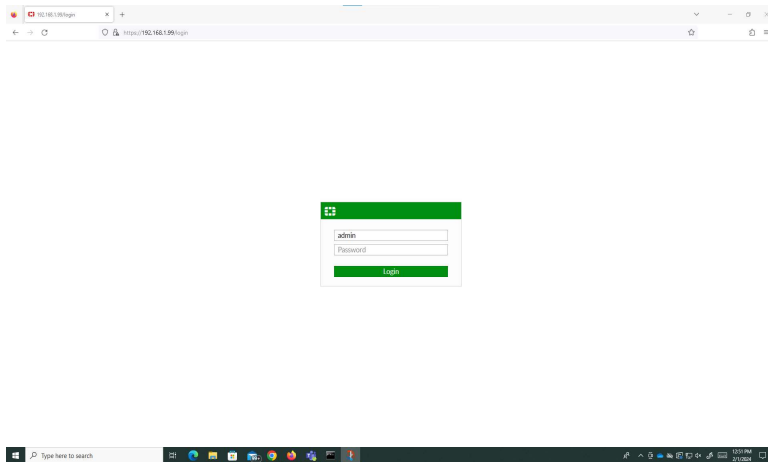
The first lab consisted of setting up the firewall, fairly straight forward as it takes you through the process to do so. The factory IP address is 192.168.1.99 and only enter the username “admin” (no password). This will make the FortiGate 40F take you through setting up the firewall from changing your password to upgrading the firmware. FortiCare will require the creation of an account while the rest of the steps are all done onboard the FortiGate. Updating from 6.4.6 to 6.4.14 puts us into the newest version of 6.4, however due to 6.4 losing support in a few months, it is wise to upgrade to a newer version, specifically 7.0, 7.2 or 7.4. This is where the second lab picks up.

The second lab had us upgrading to 7.2. We chose 7.2 over the other versions as it is the happy middle ground between being mature enough for commercial use while having a large feature set and having a few years before its end of life. Using an online upgrade path tool for Fortinet devices we were able to determine the upgrade path would be 6.4.14 > 7.0.14 > 7.2.7. Upgrading the FortiGate 40F is as simple as going to the Firmware tab and clicking on the version you want to upgrade to. It is however recommended you download your configuration before updating in case of a power outage, however since there is not much configuration on the firewall due to it being new, it should be fine to forego this step. We did face issues because we upgraded to 7.0.13 instead of 7.0.14 (didn't won't show up), this will be discussed in the problems section.




## Step by Step

1: In a browser go to 192.168.1.99, enter admin as the username.



2: Go through all the initial FortiGate Setup leaving only Upgrade Firmware left. Click Begin.



**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 ✓

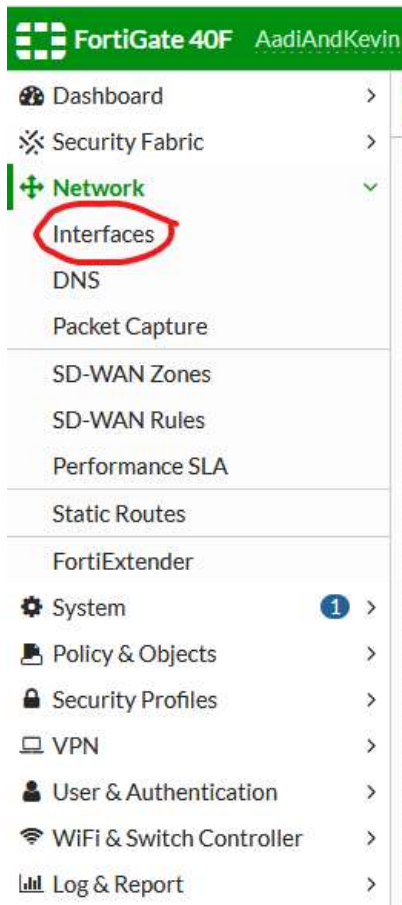
Begin
Later

3: Upgrade the firmware from whatever current version on the firewall to the latest version of 6.4 which is 6.4.14. Click Review Firmware Upgrade.

Setup Progress	Upgrade Firmware				
<p>Specify Hostname ✓</p> <p>Register with FortiCare ✓</p> <p>Change Your Password ✓</p> <p><b>&gt; Upgrade Firmware</b></p> <p>Dashboard Setup ✓</p>	<div style="background-color: #ffffcc; padding: 10px; border: 1px solid #ccc; margin-bottom: 10px;">  A new firmware version is available.         </div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;"><b>Current version</b></td> <td>FortiOS v6.4.6 build6083 (GA)</td> </tr> <tr> <td><b>Latest version</b></td> <td>FortiOS v6.4.14 build2093 (GA)</td> </tr> </table> <p style="text-align: right;"> <a href="#">Release notes</a></p> <div style="text-align: center; margin-top: 10px;"> <span style="background-color: #008000; color: white; padding: 5px 15px; border: none;">Review Firmware Upgrade</span> <span style="border: 1px solid #ccc; padding: 5px 15px; margin-left: 10px;">Later</span> </div>	<b>Current version</b>	FortiOS v6.4.6 build6083 (GA)	<b>Latest version</b>	FortiOS v6.4.14 build2093 (GA)
<b>Current version</b>	FortiOS v6.4.6 build6083 (GA)				
<b>Latest version</b>	FortiOS v6.4.14 build2093 (GA)				

4: In order to upgrade, you will need internet connection. Under network, click

Interfaces.



5: Click the Edit button.

FortiGate 40F

LAN

1 2 3 A

WAN

Create New

Edit

Delete

Search

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP F
802.3ad Aggregate						
fortilink	802.3ad Aggregate	a	Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.255
Hardware Switch						
lan	Hardware Switch	lan1 lan2 lan3	192.168.1.99/255.255.255.0	PING HTTPS SSH FMG-Access Security Fabric Connection	1	192.168.1.110-192.168.1.255
Physical Interface						
Internet (wan)	Physical Interface		192.168.41.199/255.255.254.0	PING SSH FMG-Access		

6: Set up the Fortigate 40F to use DHCP.



Edit Interface

Name
Internet (wan)

Alias
Internet

Type
Physical Interface

Role ⓘ
WAN

Estimated bandwidth ⓘ

0
kbps Upstream

0
kbps Downstream

Address

Addressing mode
Manual DHCP Auto-managed by FortiPAM PPPoE

Status
✔ Connected

Obtained IP/Netmask
192.168.41.199 255.255.254.0
Renew

Expiry Date
2024/02/01 15:31:22

Acquired DNS
1.1.1.1 8.8.8.8

Default gateway
192.168.40.1

Retrieve default gateway from server
✔

Distance
5

Override internal DNS
✔

Administrative Access

IPv4

☐ HTTPS
☒ FMG-Access
☐ FTM

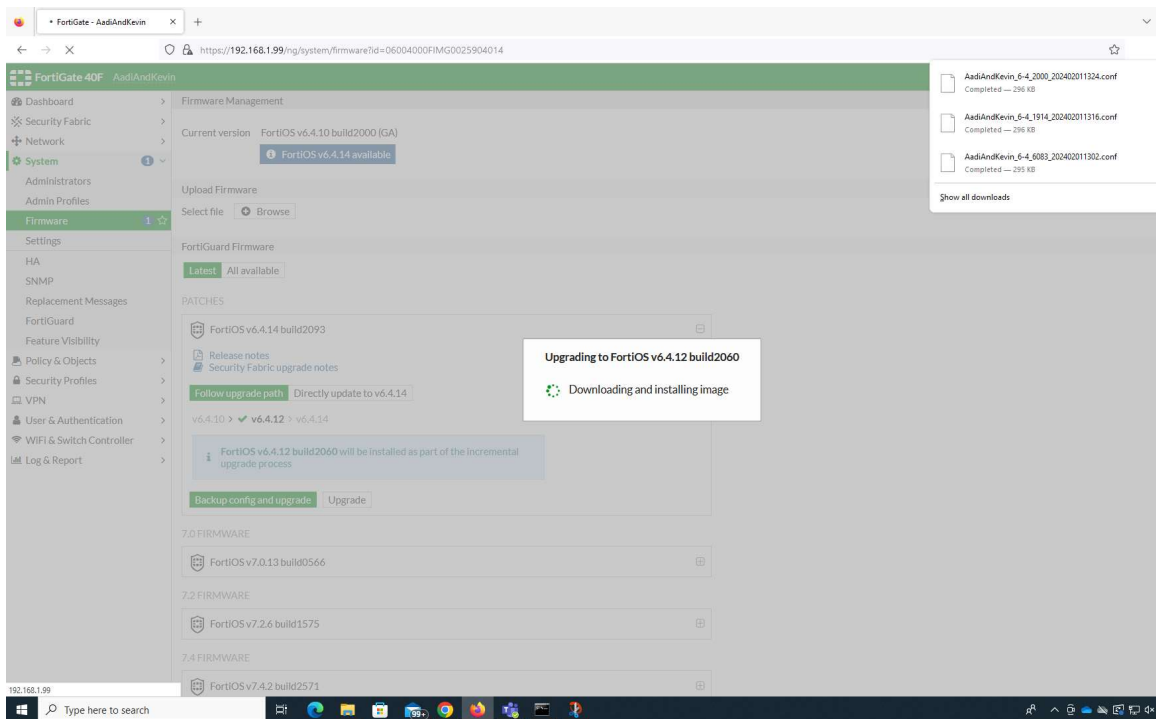
☐ HTTP ⓘ
☒ SSH
☐ RADIUS Accounting

☒ PING
☐ SNMP
☐ Security Fabric Connection ⓘ

Receive LLDP ⓘ
Use VDOM Setting
Enable
Disable


7: Go to System > Firmware and select follow upgrade path, it will ask you if you want to backup your config, we recommend that you do.


9





8: Do it again to go from 6.4.12 to 6.4.14


#### PATCHES

 FortiOS v6.4.14 build2093

 Release notes

 Security Fabric upgrade notes

 Backup config and upgrade

 Upgrade

9: Go to network > Interfaces and set the DHCP address range to shown below

Edit Interface

Name
lan

Alias

Type
Hardware Switch

Interface members
lan1
lan2
lan3

Role
LAN

Address

Addressing mode
Manual
DHCP
Auto-managed by FortiPAM
PPPoE

IP/Netmask
192.168.2.99/255.255.255.0

Create address object matching subnet

Name
lan

Destination
192.168.2.99/255.255.255.0

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
192.168.2.110-192.168.2.210

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

Automatically authorize devices

STP

Security mode

SPAN (Port Mirroring)

Traffic Shaping

The second part of the lab is upgrading to from 6.4 to 7.2, the reason be chose 7.2 over 7.0 or 7.4 is stated in the background information section.

1: Using an online upgrade path tool, this is the proper way to upgrade from 6.4 to 7.2

## Recommended Upgrade Path


Following is the recommended FortiOS migration path for your product


Version	Build Number
6.4.14M	2093
7.0.14M	0601
7.2.7M	1577


2: Go to System > Firmware and click Follow upgrade path. We recommend Backup config and upgrade for any unexpected power failures happen.

This will upgrade you to 7.0 first before you can upgrade to 7.2.

## 7.2 FIRMWARE


 FortiOS v7.2.7 build1577


 [Release notes](#)

 [Security Fabric upgrade notes](#)

Follow upgrade path

Directly update to v7.2.7

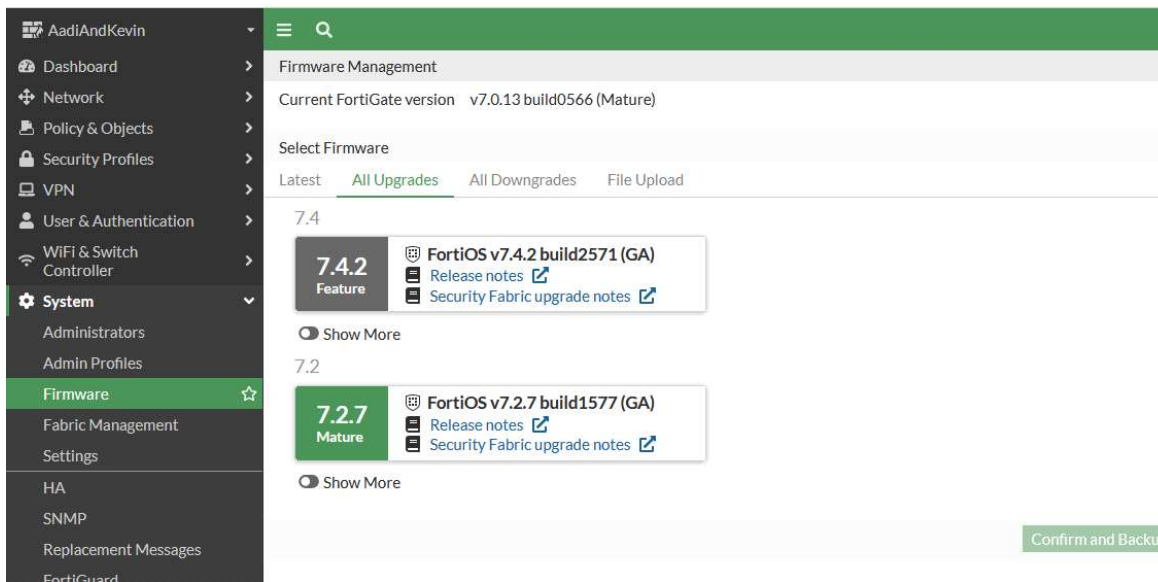
v6.4.14 >  **v7.0.13** > v7.2.7

 FortiOS v7.0.13 build0566 will be installed as part of the incremental upgrade process

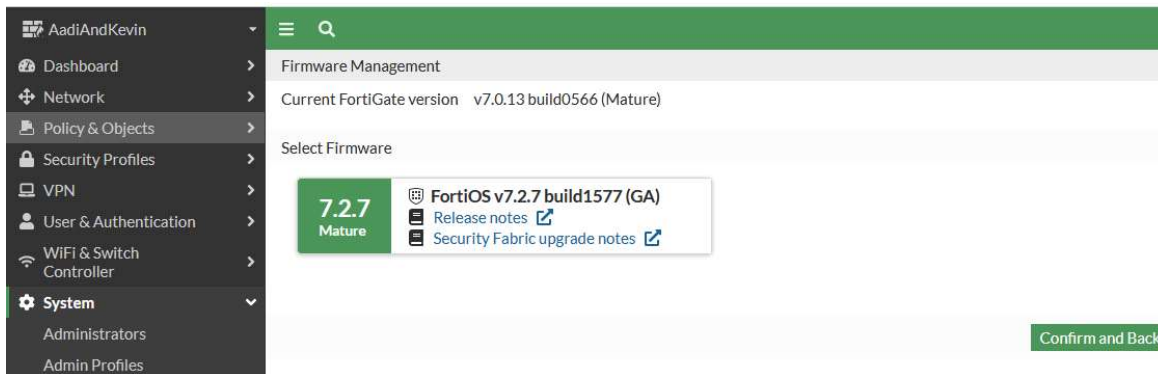
Backup config and upgrade

Upgrade

3: Once 7.0 is loaded go to System > Firmware > All Upgrades and select 7.2.7 as your next upgrade.



#### 4: Select 7.2.7 and click Confirm and Backup Config



5: This will not work as you are on 7.0.13 and the upgrade path requires you to be in 7.0.14. Upgrade to 7.0.14 beforehand then to 7.2.7



## Issues

We faced an issue while updating from 7.0 to 7.2. This was due to the fact that when we updated to 7.0, only 7.0.13 was available, we updated to 7.0.13 however there was no upgrade path forward to 7.0.14, the version we needed to be on in order to move forward to 7.2. We were able to fix this issue by waiting till the next day (likely due to a power cycle) and were able to update to 7.0.14 and proceed to 7.2.7.

## Conclusion

Though a single lab writeup, this contains two very simple set up labs for the FortiGate 40F. FortiOS seems a lot easier to use compared to Palo Alto and the initial setup and sequential updates were very easy step by step processes where the OS takes you through and even someone with very little knowledge could be able to do these tasks. Deciding between the 7. versions however would require a little more IT knowledge and research. In the end this lab was a simple set up and update like we did earlier in the year for the Palo Altos, the next lab consist of K-12 school filtering which will utilize our now set up firewall's feature sets.