Fortinet Firmware Update Lab

Emma Matsuda

Advanced Cisco Cybersecurity

**Purpose**

The purpose of this lab is to conduct research and find the best fit solution for our situation, and then physically configuring the update. Through this lab, the CCNPs were to first start up the Fortinet firewall that was provided, and then we were to research the best version to update the firewall to. We were given the choice 7.0, 7.2, and 7.4. My group and I decided to update the version up to 7.2, since version 7.0 was too old but 7.4 was too new, meaning there were multiple updates.

**Background Info**

FortiOS is Fortinet’s operating system and is the foundation of the Fortinet Security Fabric. The Security Fabri is the industry’s highest-performing and most expansive cybersecurity platform, built on a common management and security framework. It ties all of the Fabric’s security and networking components together in order to ensure seamless integration, enabling the convergence of networking and security functions to deliver a consistent user experience and resilient security posture across all manner environments.

The Security Fabric has one unified operating system that spans the entire distribution. This adds the advantages of:

* Broad reach and control across the attack surface/at every stop of the attack cycle
* Consistent and centralized management
* Orchestra of security policy and configurations
* High-performance enforcement of context-aware security policy
* AI based threat detection/recommendations.
* AL based data correlation – analysis/reporting across a unified Fabric-level dataset.
* Automated and multipronged response in real time
* Improved threat response
* Reduced risk through enhanced security orchestration, automation, and response (SOAR) capabilities

With an expansive Fortinet Security Fabris in place, organizations of any size can easily be assured that they have the tools they need to address all their security and networking challenges, no matter how broadly their users and networks are distributed.

We first started with the update to 6.4.14. The FortiOS 6.4.14 supports some new features. Some of these new features include things such as:

* Firmware upgrade notifications
* Transferring a device to another FortiCloud account 6.4.1
* FortiCare registration disclaimer 6.4.1

New features within the dashboards and widgets include:

* Consolidate Monitor and FortiView pages
* IP address tooltips
* View session information for a compromised host 6.4.1
* Consolidated dashboard usability improvements 6.4.1
* Add detachable CLI console tabs 6.4.2
* Implement a user device store to centralize device data 6.4.3

The FortiOS has been constantly upgrading, creating multiple different versions. The comparison of the 7.0, .2, and .4 versions are as below.

|  |  |  |
| --- | --- | --- |
| 7.0 | 7.2 | 7.4 |
| **End of Engineering Support\* in March 2024** (End of Support\*\* September 2025) | **End of Engineering Support in March 2025** (End of Support September 2026) | **End of Engineering Support in March 2026** (End of Support November 2027) |
| expands the Fortinet Security Fabric’s ability to deliver consistent security across all networks, end points, and clouds with SASE and ZTNA (+ etc.)  expands visibility and control.  ensures the consistent deployment and enforcement of security policies.  enables centralized management across the entire distributed network.  allows organizations to run their businesses without compromising performance or protections.  supports seamless scalability.  simplifies innovation consumption. | inline sandbox that transforms a traditional detection sandbox capability into real-time in-network prevention  advanced device protection that automatically discovers and segments OT and IoT devices  further unifies the convergence of networking and security across NGFW, SD-WAN, LAN Edge, 5G, ZTNA, etc.  enhance support for Fortinet Security Fabric and its ability to consolidate security point products.  A Dedicated IPS that enables migration from separate hardware to NGW while preserving operations and compliance practices. | unified management and analytics across hybrid networks  hybrid mech firewall for data center and cloud  secure SD-WA for branch offices  single-vender SASE for remote users and branch offices  universal ZTNA for remote users and campus locations  WLAN/LAN for branch offices and campus locations  SOC augmentation and automation with FOrtiAnalyzer, FortiSOAR, FortiSIEM, and FortiGuard SOC-as-a-Service |

End of Engineering Support\* = The date beyond which Fortinet no longer commits to provide engineering support for the software. The software enters a *must-fix* support phase after this date, during which, maintenance builds will only be produced for industry-wide critical issues and PSIRT vulnerabilities. EOES dates are generally about 36 months after the GA date.

End of Support\*\* = The date when Fortinet will no longer sell, manufacture, or improve the product after this date and is under no obligation to provide support services. In general, the EOS takes place as below:

* Hardware – 60 months after EOO date
* Software – 54 months after the GA date
* Stand-alone Services – on the service contract termination date

**Lab Summary**

1. Start up the Fortinet firewall, connecting the Fortinet port to the computer
2. Enable DHCP and set up the computer accordingly to configure settings on the web GUI
3. Access the web GUI
4. Research the version updates
5. Update the firewall to the version selected

**Lab Commands**

No new commands were introduced during this lab, since everything was done in the Fortinet web GUI.

**Network Diagram/Topology**

There are no diagrams/topologies for this lab, since all of the configurations were made in the web GUI – in which they were all for simple configurations to the firewall itself.

**Configurations** – screenshots of the process

|  |  |
| --- | --- |
| 1. Console your computer into Port 1 of the Fortinet firewall |  |
| 1. Enable DHCP on computer.   (or set the IP to 192.168.1.1 255.255.255.0) |  |
|  | 1. Enter <https://192.168.1.99> to access the Web GUI for the firewall. |
|  | 1. Enter the username “admin” and keep the password blank to login. |
|  | 1. Change the password to anything you’d like. Keep the old password blank, since there was none assigned at default. We set ours to “Admin123” |
|  | 1. Then, the next screen will be the FortiGate Setup. 2. This process would allow the user to specify hostname, register with FortiCare, change Password, Upgrade Firmware, and complete the Dashboard Setup. |
|  | 1. Specify the hostname – we named our firewall “fortigate-40f16” because the device 40f is the version of the model, and our FortiGate was numbered 16. |
|  | 1. Register with FortiCare – we skipped this step initially to get our administrator to sign in for us, but this step is something we can come back to later. 2. FortiCare only for remote management |
|  | 1. Choose the optimal option for the dashboard – this will give a set of the popular, most used defaults dashboards and FortiView monitors. |
|  | 1. Once successfully logged in, the default dashboard should show up. |
|  | 1. Notice that you can see the Firmware 6.4.6 version on here. |
|  | 1. The option for the firmware version is also available to see under Systems -> Firmware. |
|  | 1. Under the same options, there is an option to “Upload Firmware,” where you can upload a file to update Firmware versions. |
|  | 1. This message will pop up, click continue. |
|  | 1. The System will reboot while updating. |
|  | 1. Under “All Available,” choose the version that you would like to update to. |
|  | 1. The System Information shows the current version – we first updated it to 6.4.14 |
|  | 1. We ended up updating it to 7.2.7, because we thought that 7.0 was too old and the EoES support date was too recent, but 7.4 had numerous updates to the version because of its bugs that were being found on the way. |

**Problems**

Although we didn’t have many problems, here is the one problem we had:

* The versions that we downloaded didn’t work for us. The file was invalid and not uploading, but to fix this, we decided to re-download all the versions and it worked fine the second time. We don’t know what was wrong with this one since we didn’t change anything.

**Conclusion**

Through this lab, we learned how to research about a Fortinet firewall and apply the knowledge to the unique situations. This is important because we will be able to apply this to different real-world situations. Along with this, we learned how to navigate through the web GUI, since this Fortinet firewall is a new device for us. We learned how to get the hang of navigating through a web GUI through the process of updating versions. We were able to nurture problem-solving skills and also the skill of being introduced to a new hardware and being able to utilize it perfectly fine.