Brit Stevens 2/3/24

Fortinet Firmware

Updates

**Purpose:**

The purpose of this lab was to introduce us to a new firewall and how it operates after learning the basics of another company’s firewall. It gave us an understanding of how to update the firmware in the Fortinet firewall with its FortiOS upgrade path and how to decide which versions are secure and get comfortable with the new GUI (Graphics User Interface).

**Background Information on lab concepts:**

* **Fortinet:** A company that specializes in cybersecurity, networking, and network security. They have over 730,000 users and is very trustworthy as a company.
* **FortiGate:** A firewall created by Fortinet that utilizations prebuilt filters that can be enabled or disabled at any time to protect from a wide array of security threats such as viruses, DNS spoofing, malware, and intrusions prevention for example. These filters are created from standard processes for cybersecurity companies of databasing threats.
* **Threat Intelligence Feeds:**
  + Most cybersecurity companies utilize Threat Intelligence Feeds which are a mass of data collected from public feeds, dark web monitoring services, and their research into threats. These are then put into threat intelligence feeds to report found malicious websites, IPs, or domains and block them.
* **Machine learning Algorithms:**
  + Companies like Fortinet use Machine Learning Algorithms to analyze internet traffic to find patterns in that traffic. These patterns can be identified and added to the TIFs if they have malicious natures.
* **Customer feedback:**
  + Although it may not seem like it, Fortinet does listen to what customers report and if many reports are around the same malicious source it will be investigated by expert Analysis.
* **Telemetry Data:**
  + Similar to customer feedback cybersecurity companies look at their Telemetry Data which is created by an automated process collected by your systems. It can be configured to collect different sources of data like all logs metrics, events, etc. from a range of devices that are connected to their servers.
* **FortiOS:** This is the OS of all Fortinet devices that is frequently updated and patched. There are different categorizations that correlate with the age of the version. When a file is very old it is known as mature because it has all of the bugs patched out which its many subversions. When a file is very new it is known as not mature due to its lack of patches. It is not recommended to use brand-new versions due to bugs they have that have been patched or sometimes even discovered. Around six months is when a file goes from not mature to mature.
* **WAN vs. LAN:** 
  + **WAN:** An acronym for Wide Access Network, is a network that spans many local networks. This is how offices connect and a user can communicate from one location to another far away. This could be across the street or in different countries.
  + **LAN:** An acronym for Local Area Network, is a network that stays within a subnet. This means it includes all many different devices like User devices, switches, routers, access points, etc. that reside within a building on the same network. You could go from your IT department to administrative through your LAN for example.

**Lab Summary:**

Before starting we had to figure out how to update the firmware of the firewalls safely. To do this we researched and created this guide:

1. Plug in the firewall and wait until the PWR light comes on.
2. Attempt to access the GUI using the default address of 192.168.1.99 and change your desktop address to be in the subnet of that IP.
3. If not successful use steps 4-6, if successful skip until step 7.
4. Access the CLI of the FortiGate to view its default management IP using the console port.
5. Type “show system interface” to view the IP set on the firewall.

If there is no IP set use the following commands to set an IP on port 1.

config system interface

edit port1

set mode manual

set ip 192.168.1.1 255.255.255.0

set allowaccess http https ping SNMP ssh

end

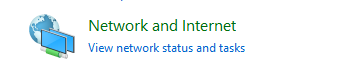
1. Now attempt to access the Gui again.
2. Login with the default credentials of “admin” and a blank password.
3. To determine the upgrade path go to <https://docs.fortinet.com/upgrade-tool> and enter your firewall model, starting operating system, and operating system you want to go to. This will tell you the file you need to download.
4. For our chosen version download the firmware image file of 6.4.8, 6.4.10M, 6.4.12M, 6.4.14M from the Fortinet Technical Support website, https://support.fortinet.com.
5. Go to System > System Information.
6. In the Firmware Version field, click the Update link.
7. Or click the Browse button and locate the lowest firmware image file first.
8. Click the OK.
9. Click the Update. Your browser uploads the firmware image file to FortiDB, which upgrades to the new firmware version and then restarts. This process takes a few minutes.
10. Repeat sequentially until up to date with 6.4.14.
11. You are now fully up to date.



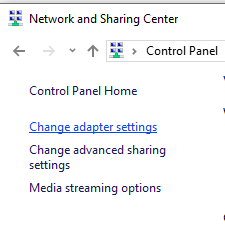
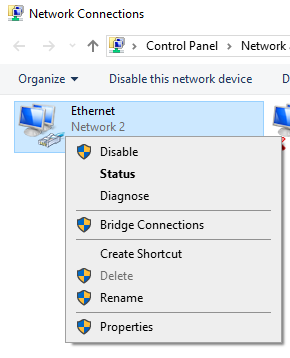
Now that we know how to set it up, cable as shown with port one connected to your PC to allow configuration.

Enter the default IP address or newly set IP to your web browser, then begin the FortiGate setup. If the webpage does not appear set a static IP on the PC. To do so type “control panel” into your search bar and open it.

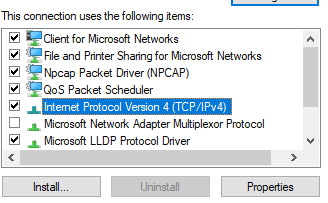
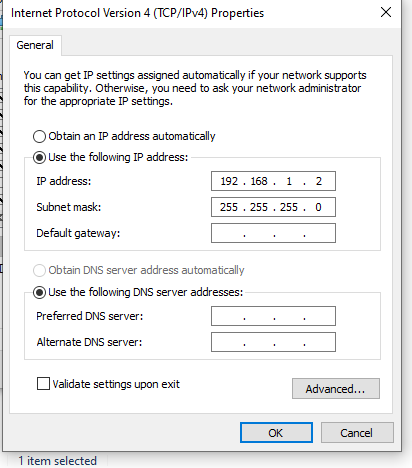




Click view network status and task.

Click Change Adapter Settings and then right-click the NIC (Network Interface Controller) being connected to the firewall and click Properties. For us, that is our only Ethernet adapter.

Scroll down through the list of connection items and find the IPv4. Once selected click properties then change an IP to be in the range of your firewall’s port’s IP. You should now be able to reach the webpage.

A screenshot of a computer

Description automatically generated

Go through the guided process of the FortiGate Setup by clicking Begin.

A screenshot of a computer error

Description automatically generated

Change the hostname to any preferred name of your choice, Then press ok.

A screenshot of a computer screen

Description automatically generated

Select Optimal for the Dashboard setup.

A screenshot of a computer

Description automatically generated

Now you are in the GUI, note that the firmware build is 6.4.6. Next, we will update the firewall to reach up to 6.4.14.

A computer screen shot of a computer

Description automatically generated

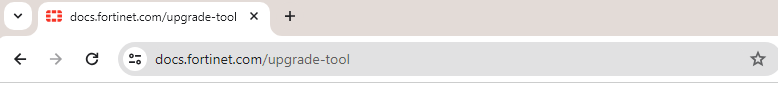
Next, open a new browser tab then head to support.fortinet.com, then now we will set up an account to get the files for the updates.

A screenshot of a computer

Description automatically generated

Register an account with Fortinet so that you can receive the firmware update packets. Then go to support and then choose Firmware updates to find the packets needed to update the firewall.

We did not go through this process as all of the firewalls in our lab were registered under our instructor account.



This website will help you find the update path required for the firewall to update the firmware properly.

A screenshot of a computer

Description automatically generated

This update path will allow the user to update from 6.4.6 to 6.4.14. the specific reason we have to use this update path is so that the system is not at risk of losing its configuration from a faulty update from an incompatible version to another newer version.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

In the GUI go to settings then click on Firmware Management and upload the files that you had downloaded early. Update the firewall in order of the upgrade path to ensure no faulty configurations.

A screenshot of a computer error

Description automatically generated

Once this message pops up click continue to confirm that you are updating the firmware.

A screenshot of a computer

Description automatically generated

This is what you will see once the firewall is in the update process. Once the update is complete, repeat the process until you reach the firmware version of 6.4.14 using the given upgrade path on the upgrade path tool.

A screenshot of a computer

Description automatically generated

When complete, log into the firewall and check system info to see if the firmware is updated to 6.4.14. This will confirm the updates have worked properly.

A screenshot of a computer

Description automatically generated

You can see system information here.

Next, we will determine what version we will upgrade to next for the purposes we’re using the FortiGate.

|  |  |  |  |
| --- | --- | --- | --- |
| 7.0.0-13 | 7.2.0-6 | 7.4.0-2 | |
| **FEATURES:**   * 7.0 has no DDoS protection or security events overview * 7.0 must use CLI for automatic Web URL filtering. This would make it more difficult to configure. | **FEATURES:**   * Has logging capabilities and new security events page for greater overwatch. * Has DDoS prevention by banning persistent IPs even through power cycles. * automation stitches which help with logging violations. * Can use the GUI to configure URL filtering. * prevention of DHCP snooping, each switchport Mac address can only have 1 IP address, better layer 1 security. * More VPN services on 7.2.0 than 7.0 | **FEATURES:**   * Simplified automation trigger from 7.2.0 meaning easier configuration. * Real-time file system integrity checking has two main purposes:   Prevent unauthorized.  modification of important binaries.   * Detect unauthorized binaries and prevent them from running. | |
| **DIFFERENCES:**   * End of engineering support in March 2024, will no longer receive patches and bug fixes * Known vulnerabilities 7.2.4 and under that have not been patched | **DIFFERENCES:**   * Has been out for almost 2 years, and is a mature version. * Still has support from Fortinet. * Reported to have greater user stability than 7.0 versions. | **DIFFERENCES:**   * 7.4.0 is not mature, less than 6 months old at the time of writing, and could still contain critical faults |

<https://www.ge.com/content/dam/cyber_security/global/en_US/pdfs/2023-10-19_FortiOS_7.2.4.pdf> (vulnerabilities).

We decided 7.2.6 is the best version for us after research which would be best for us in our lab scenario of a school district monitoring web traffic from users.

(after we did our research 7.2.7 was released and we updated to that version).

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer error

Description automatically generated

Using the same process as before update to 7.2.6. now.

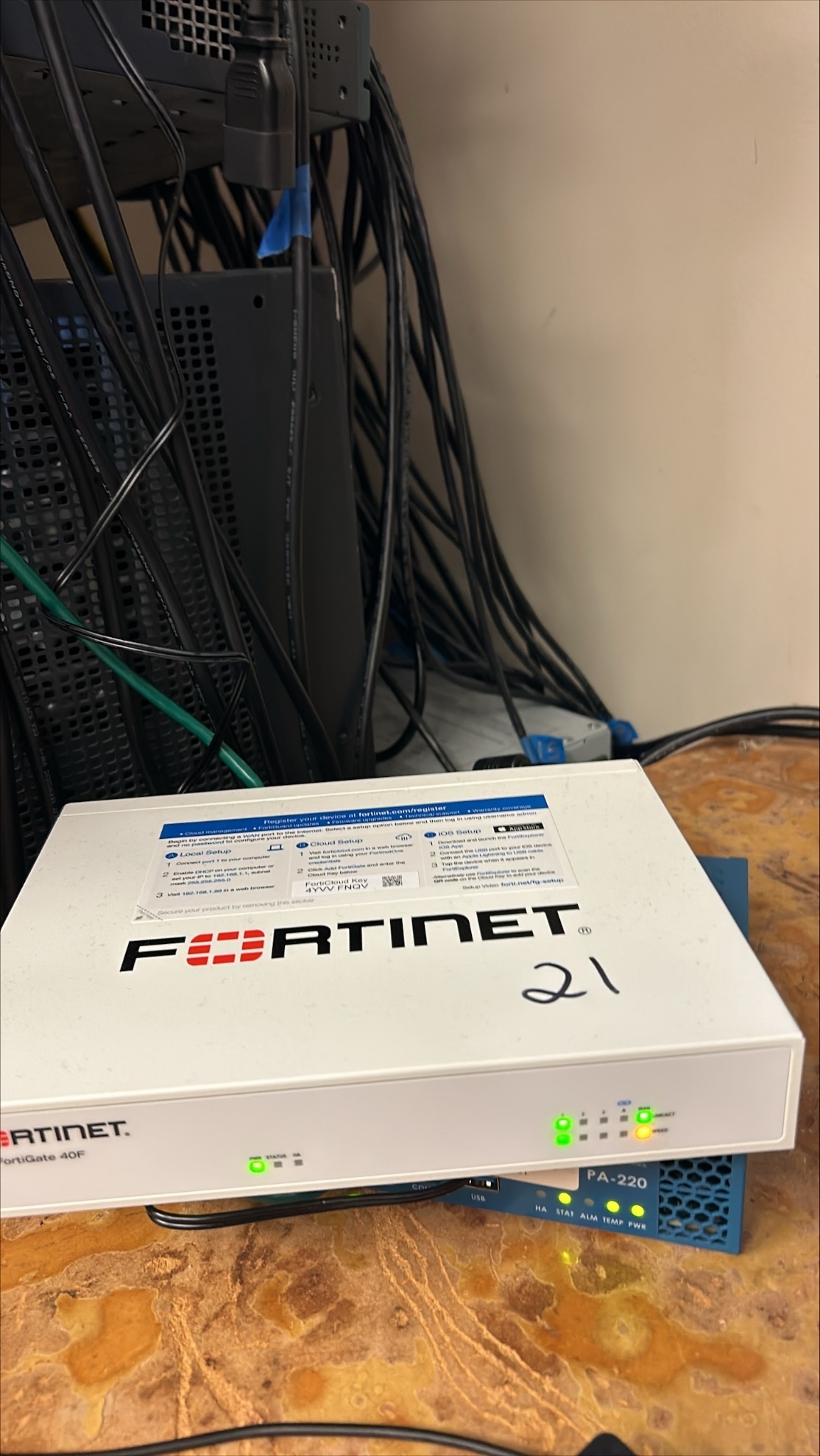
A screenshot of a video game

Description automatically generated

Here we can see we are on a new version. Instead of a FortiOS 6.X version welcoming we have a FortiOS 7.2 welcoming message.

A screenshot of a computer

Description automatically generated





We will now connect the FortiGate to the internet as shown. Connect the WAN port to your router that goes to the ISP and the internet. The WAN port LED should now to green to show it is up.

A screenshot of a computer menu

Description automatically generated

Go to Network then to Interfaces where we will assign the IP to the WAN.

A screenshot of a computer

Description automatically generated

Select your WAN physical interface then choose Edit.

A screenshot of a computer

Description automatically generated

This is the Edit interface that we will use to configure the DHCP (our ISP gives addresses through DHCP but your ISP may differ on how or if addresses are distributed). note the Default gateway is 192.168.40.1.

A screenshot of a computer

Description automatically generated

Next, select Static Routeon the left navigation panel then choose Create New. Leave the Destinationas 0.0.0.0/0.0.0.0, this will send all traffic out the interface we set it to. Set Interface to WAN and put a comment to document what route is meant for, this allows for easier future reference and excellent documentation. Ensure that the Gateway Address is using the previously noted Gateway Addressof the router (192.168.40.1 in our case), click ok to confirm settings.

A screenshot of a computer menu

Description automatically generated

Next, navigate to Policy & Objectsthen select Firewall Policy.

A screenshot of a computer

Description automatically generated

Confirm that your LAN to WAN policy is configured properly.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

If needed edit the policy as shown above to allow the inside network to be able to communicate to the internet.

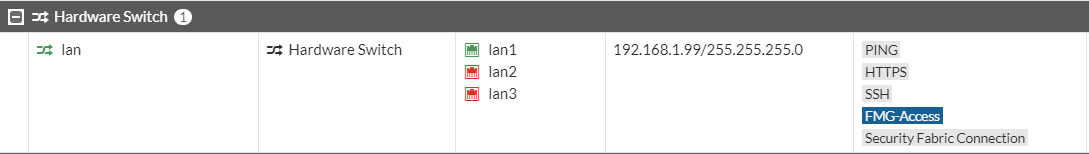


A screenshot of a computer

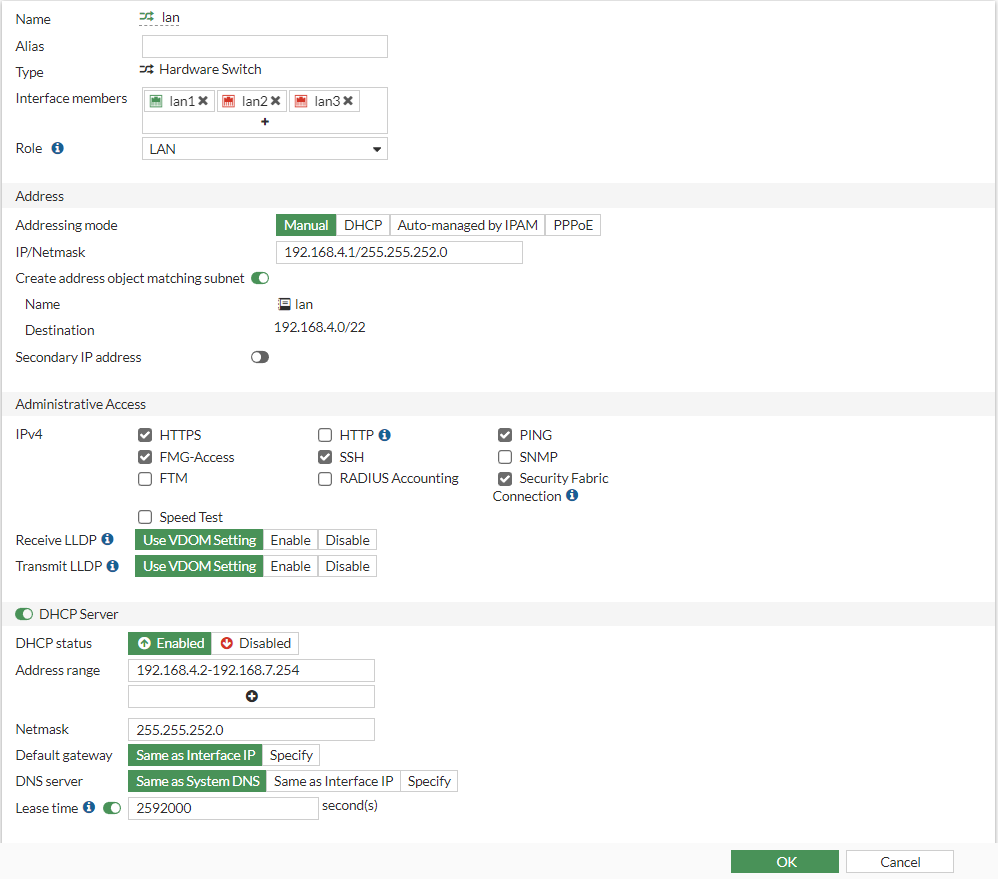
Description automatically generated

You should now be able to access the internet through the firewall. One website is from another country while the NYT games site is a US website.

Now that we are at this step we can configure for a school district scenario in the next lab.

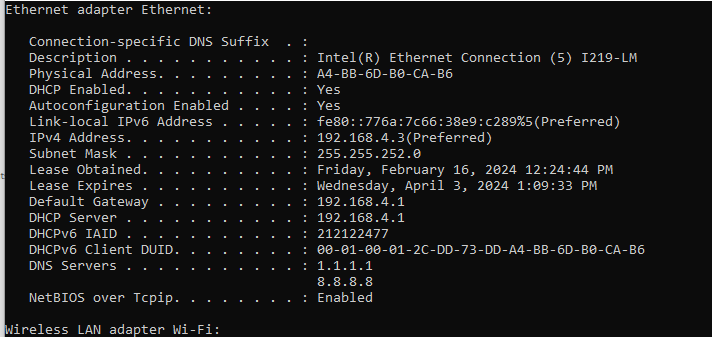


There is one more step although not necessary which is to set up a DHCP pool for the inside network. Our firewall functioned without an inside network DHCP pool because we statically set an address on the PC but this can be very inefficient if you have many devices wanting to be on the network. First, go to network -> interfaces and select Lan. Right-click to edit.



We will edit the IP address of the lan1 interface since leaving any configurable addresses or logins as the factory defaults is a security risk as they are easily found on the internet. We set our FortiGate to 192.168.4.1 with a subnet of 255.255.252.0 which is the address pool we will use for our DHCP pool given to the Inside network. This allows 1022 usable addresses in the network which is what we are saying is the size of our imaginary school district for our lab. This subnet can be whatever you want but we chose one optimal for our future scenario.

Toggle the DHCP Server option to on and select Enable to allow the port to give addresses to all connected devices in the range we set. Type in your desired usable address range in the corresponding box. Use a subnet that contains that entire range or else there will be errors. Leave the default gateway and DNS server as default and configure your Lease time to a reasonable time like 2592000 seconds (30 days). We chose this since our school district will not have devices added often. Select ok at the bottom of the screen to confirm changes.



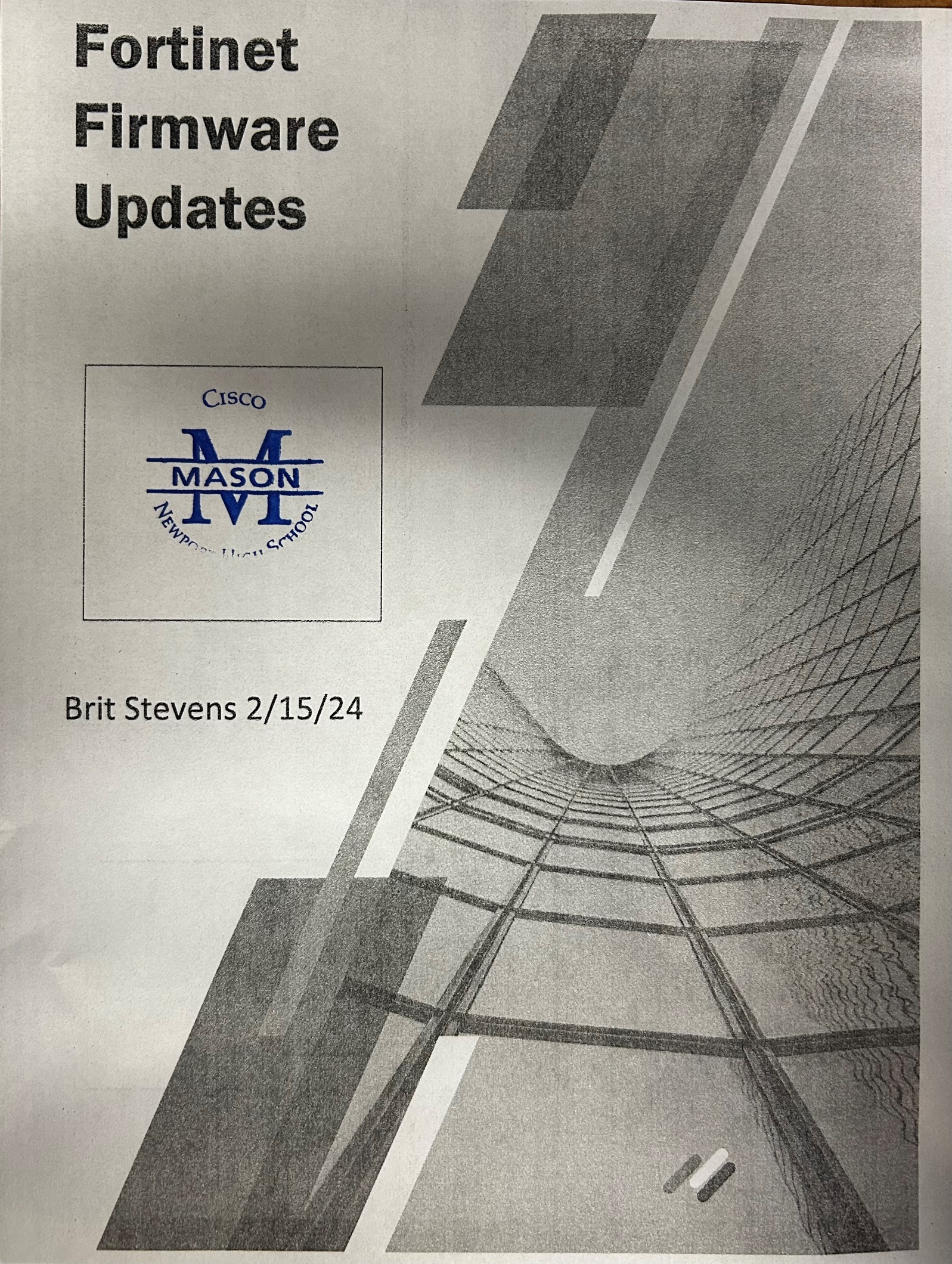
Once the changes process you will lose connection to the firewall as you are now entering an invalid address to reach it with the previously statically set address. You must go back and repeat the steps of changing the IP address of the ethernet interface only we select DHCP over Static this time. Enter your new management address of the firewall into the web browser to confirm changes. You may also go into your command prompt and confirm your IP address changed. Use the command “ipconfig /all” and scroll until you see the applicable ethernet adapter connected to the firewall’s DHCP range. If the IP is not an IP in the range of the DHCP pool use the command “ip config /renew” and wait until the command processes. You should now be able to access the firewall again.

**Problems:**

* Could not download update files as we did not have the firewalls registered to our account.
  + The instructor downloaded the firmware updates we needed and passed them to us.
* DHCP pool out of range of firewall interface, could not access the firewall.
  + Set static IP to access and reconfigured pool.
  + Additionally forgot to turn off static IP and could not access the firewall occasionally.
* Fewer guides than PaloAlto firewalls.
  + Researched using owner manuals and figured out the steps ourselves.

**Conclusion:**

Overall this Lab was very interesting because it taught us about file versions and which ones are optimal based on factors like age, use cases, etc. Previously he had learned how to configure PaloAlto firewalls which are much harder to configure and not as optimized as the Fortinet GUI was. I found that I much prefer Fortinet firewalls to Paloalto given that in general they have the same feature and FortiOS is very user-friendly. That said, this lab was easier to understand than previous ones because of our experience on the PaloAlto and helped strengthen that understanding of the concepts and similar configurations. I think the biggest takeaway I have from this is the understanding of how firewalls work and how the process of first setting them up is similar between companies and devices. Knowing how to set up one is very beneficial when you have to configure a new device that has differences but overall is very similar.

****

