ASA 5505

*CISCO Firewall Factory Reset and SOHO*

Adv Cisco Cybersecurity – Lab 6

Jason Liu

Cybersecurity – Mr. Mason & Mr. Hansen

Period 5

*Lab 6: CISCO ASA 5505 – Factory Reset and SOHO Configuration*

**Purpose**

The objective of this lab is to factory reset and set up a Cisco ASA 5505 firewall for a Small Office Home Office (SOHO) configuration. Configuration should be accessed through Adaptive Security Device Manager (ASDM) and its respective Java environment version and launcher. Another objective is to record all problems encountered in this lab, and document all attempted solutions for future reference.

**Background Information**

Released back in 2005, the Cisco Adaptive Security Appliance (ASA) 5500-x Series Firewalls were a popular lineup known for its early representations of Next-Generation firewalls, with integrated cloud and software-based security services, including Application Visibility and Control, Web Security Essentials, and Cisco Cloud Web Security. They also kept pace with evolving technology by combining the visibility from local traffic with in-depth global network intelligence through Cisco proprietary services like TrustSec, AnyConnect (for mobile client insight), Security Intelligence Operations, and other services. This entire series, including the 5505, has reached end-of-life on August 31st, 2022.

The Cisco ASA 5505 is the smallest and most SOHO-friendly device with a compact 8 port design. Although it is no longer supported by Cisco, it still runs many integrated features that can be utilized for simple SOHO connection. Configuration is done via the Adaptive Security Device Manager (ASDM) or more basic commands, including show commands, via the Cisco CLI. The ASDM launcher software must be downloaded directly from the ASA firewall and can be accessed by entering the address of “https://<*ASA-Address*>/admin” in a browser. This is similar to entering a webGUI of modern firewalls, but this one leads to a download page for the launcher rather than a configuration page. The default management IP is 192.168.1.1, and the address should be reachable from the PC that is used.

A main feature advertised by this firewall was the Cisco ASA Botnet Traffic Filter. Botnets are malicious software installed on endpoints and controlled by another entity through a communications channel such as IRC, peer-to-peer, or HTTP. Back during the increase of web applications like Facebook and MySpace, the possibility of an endpoint being infected had increased greatly and Cisco responded by releasing the Botnet Filter to provide long-term infection prevention systems, visibility, and endpoint remediation. Traffic Filter Reports are also available on the ASDM.

All the information above is researched from the main Cisco publication and its associated whitepaper documents. The site can be found here:

<https://www.cisco.com/c/en/us/support/security/asa-5505-adaptive-security-appliance/model.html>.

**Lab Summary**

This lab is incomplete. However, as a record for documentation purposes, all steps will still be documented.

First, console into the firewall. The PuTTY application was used here. On the CLI, attempt to factory reset the firewall by entering global configuration mode and entering the commands: “config factory-default” and “reload save-config noconfirm”. It is also possible to view the version of the ASA using the show version command on the CLI.

Then, changing the PC address to be in the same subnet as the management IP address of 192.168.1.1, we attempted to enter that address into a browser. Mozilla Firefox was used. The webpage prompted to enable TLS 1.0/1.1, accept risks, and continue. It led to a download page, one link for downloading the proper java runtime environment, and another link for the executable file (.exe) for the ASDM launcher. Running the executable file, an ASDM shortcut icon appears on the desktop, as well as an executable .jar file under Program Files x86 > Cisco Systems, which both opens what appears to be the same application – the ASDM.

When entering the management address into the prompted screen of the ASDM, it would load with many errors. The most progress made was entering the ASDM, but the loading bar for accessing the configurations would be stuck at 17%. This specific number of 17% appeared in all our troubleshooting attempts and was the most progress we could make. Because we cannot access the ASDM, we cannot configure the firewall. Specific details on problems and attempted solutions can be found in the *Problems* section.

**Lab Commands**

The CLI commands used for this lab are familiar and intuitive as it is considered a Cisco CLI. The following commands were used:

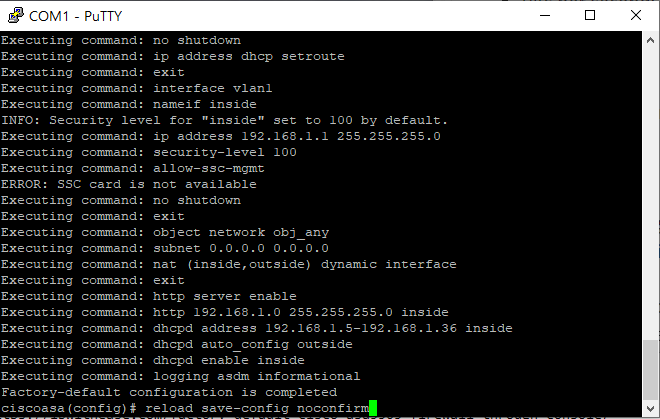
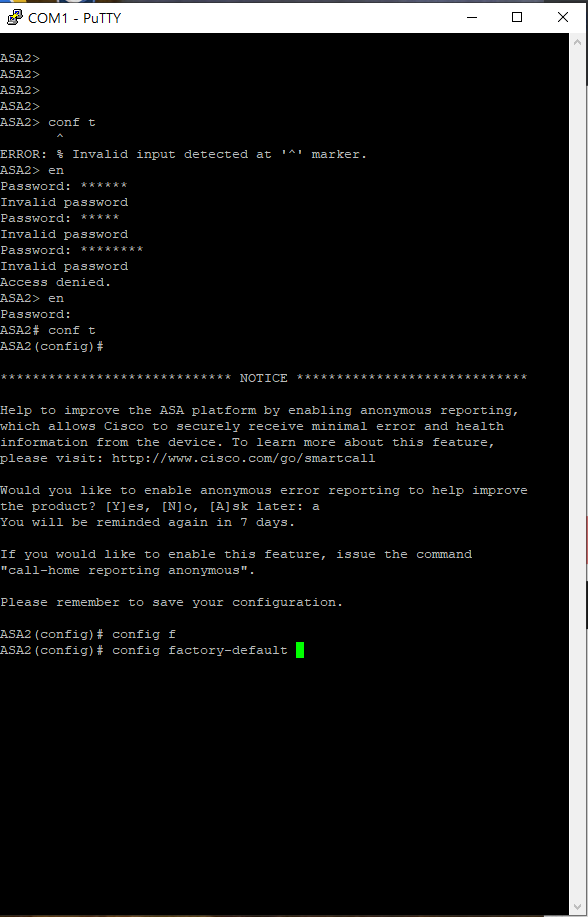
**show version** *–* Check the version of the firewall.

**enable** *–* Enters *enabled* mode.

**configuration terminal** or **config t** *–* Enters *global config* mode.

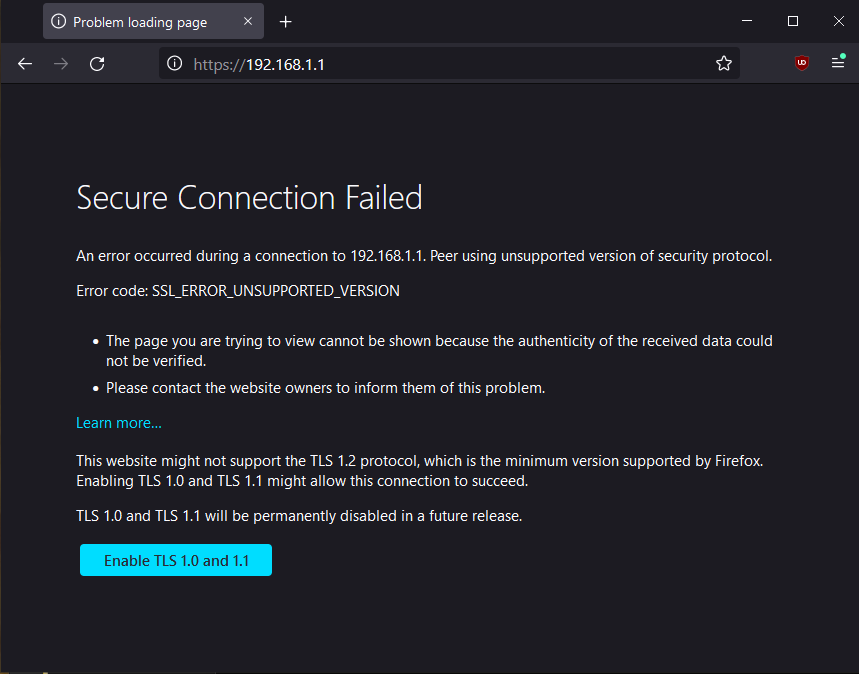
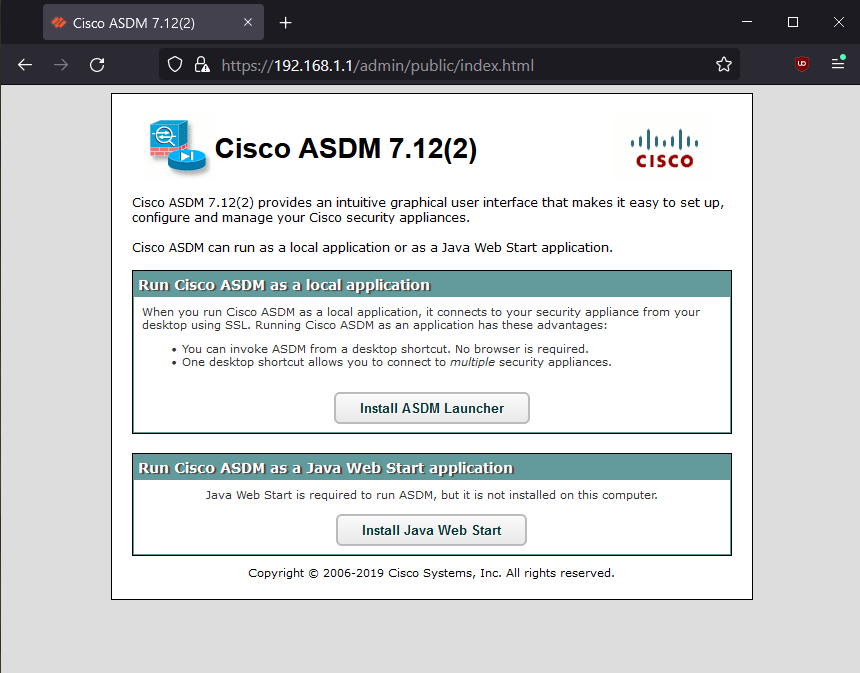
**config factory-default** *–* Resets firewall configuration settings; factory reset.

**reload save-config noconfirm** *–* Reloads/reboots the firewall to reset it.

**Procedure**

Console into the CLI and use PuTTY.

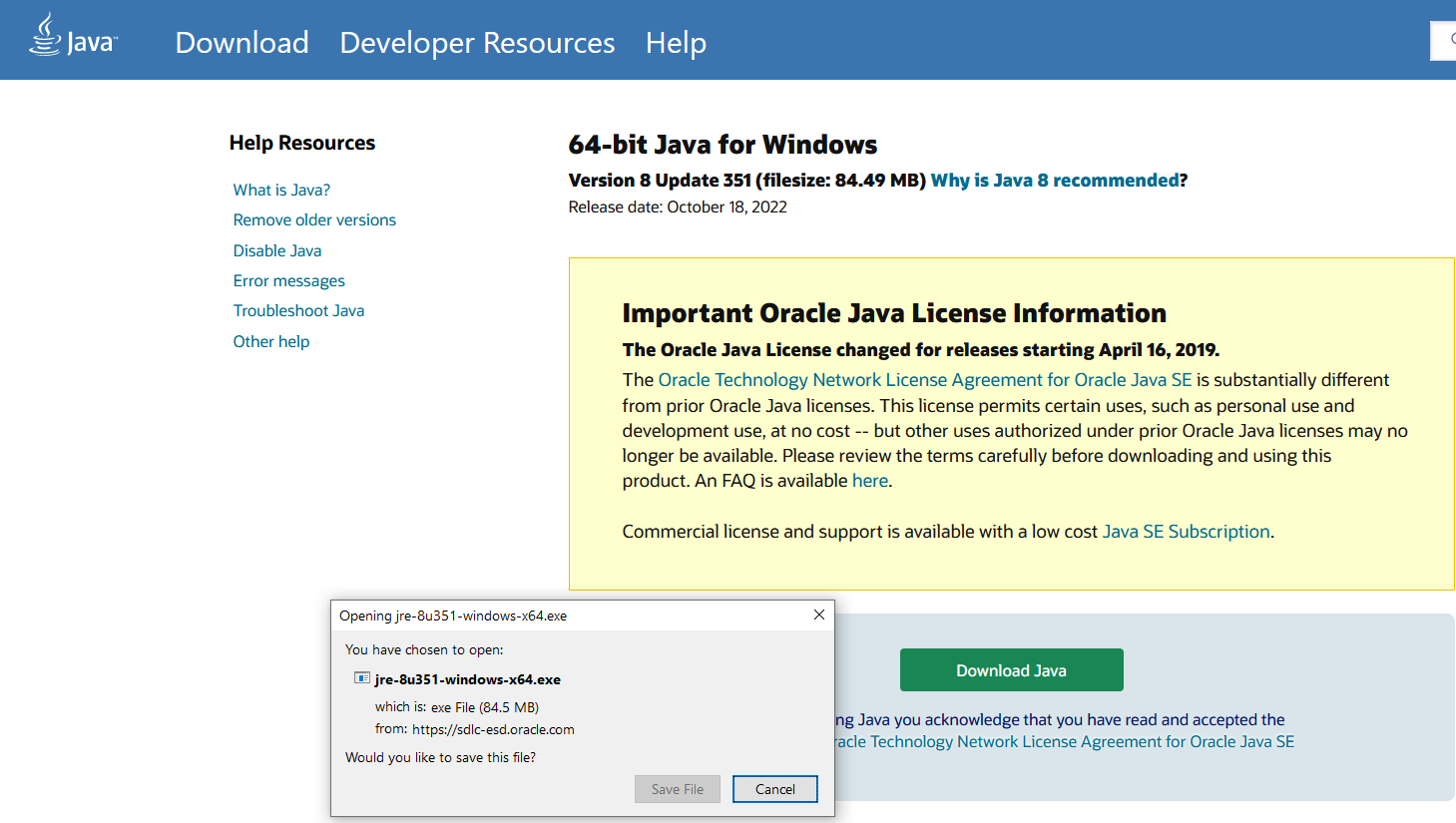
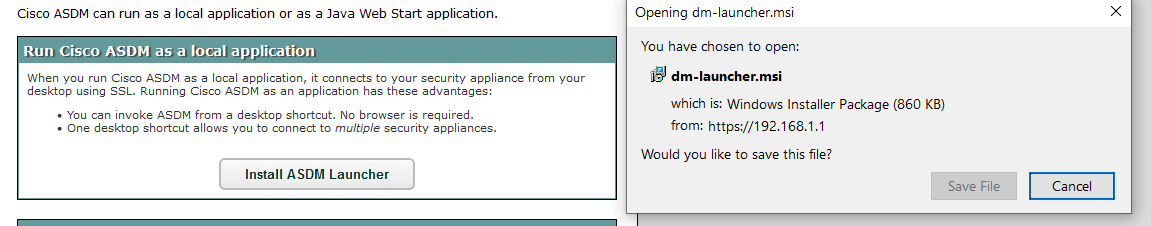
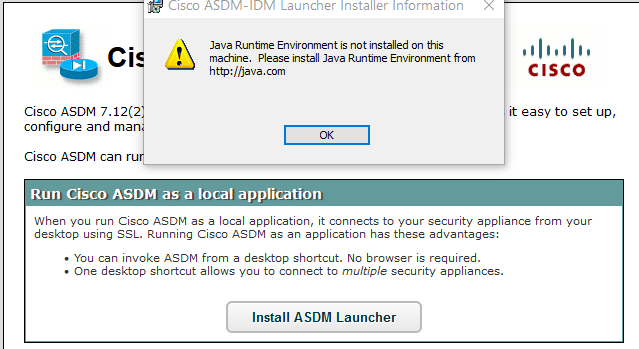
Reset password after default credential – *admin* – for both fields. Factory Reset using the CLI and the two commands (see *Lab Commands*).

****

The ASDM download page appears.

Access the management IP address via a browser. Mozilla Firefox was used.

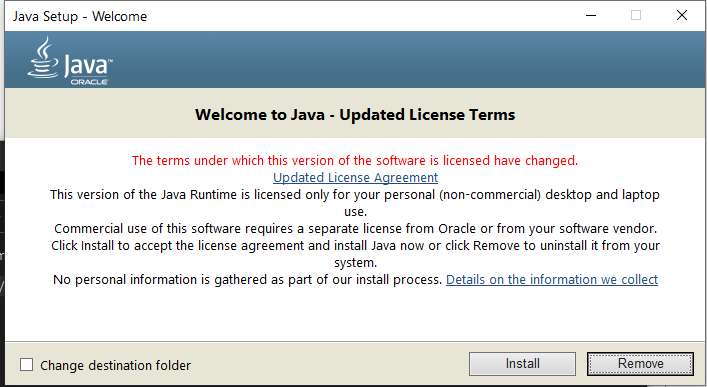
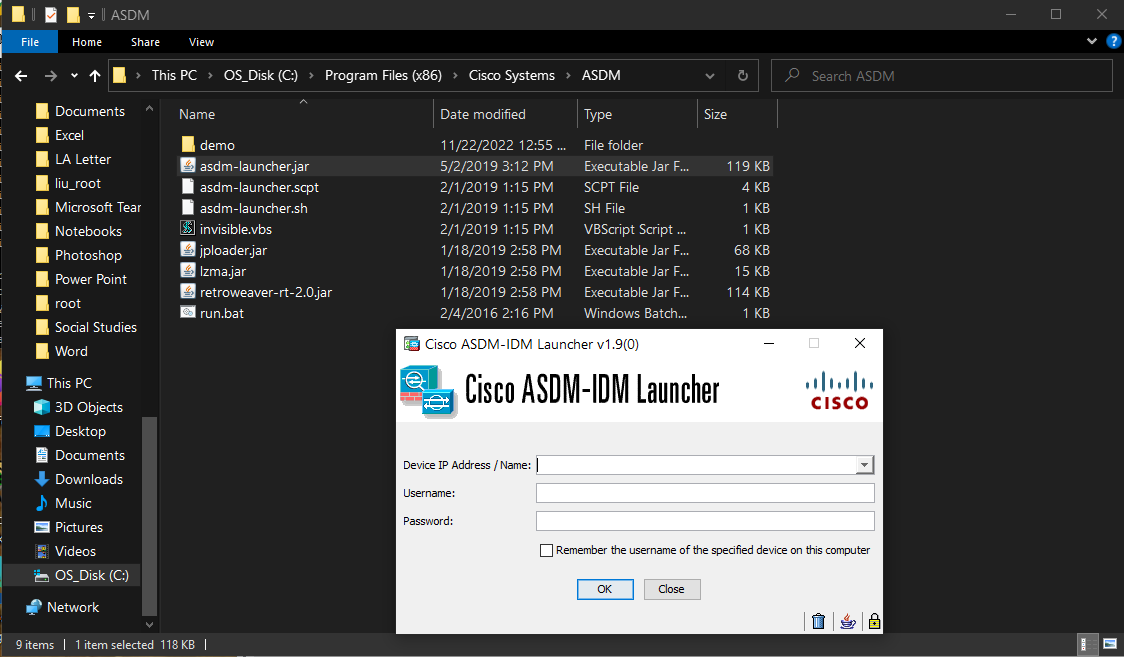
Enable TLS to enter the page.

****

Downloaded Java version 8u351 (version 8) for Windows x64.

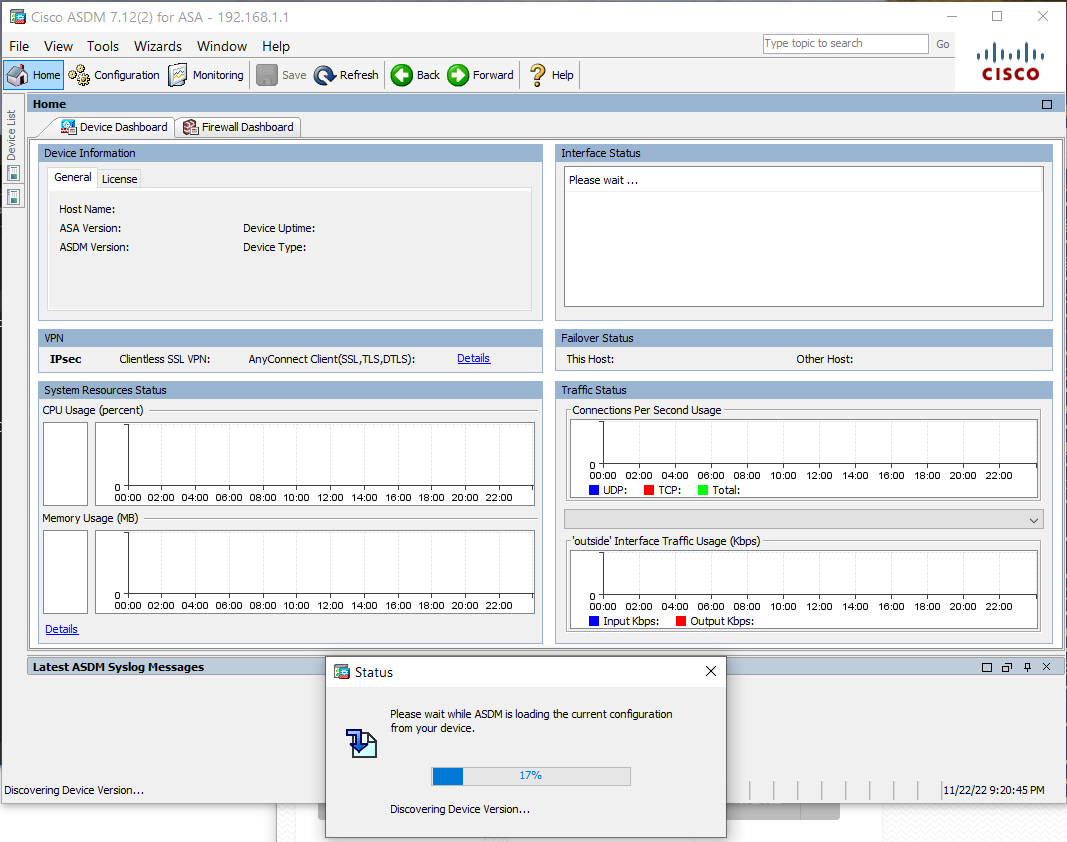
Java is required. Follow the Java Web Start link. It will lead to the Java Runtime Environment Download page.

Download and run the Device Manager launcher. This downloads the ASDM.

****

Open the ASDM-IDM launcher via the executable Jar file. It will ask for the device IP.

Java successfully downloaded.

****

After entering the default device IP of 192.168.1.1, a template of the ASDM is shown.

There are issues with loading and displaying the current configuration, where the status bar only loads to 17%. Future configuration cannot be done.

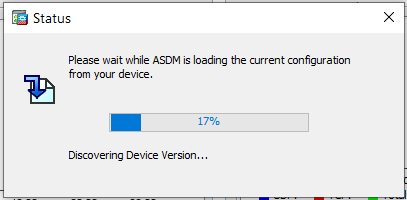
See *Problems* section for more details.

**Problems**

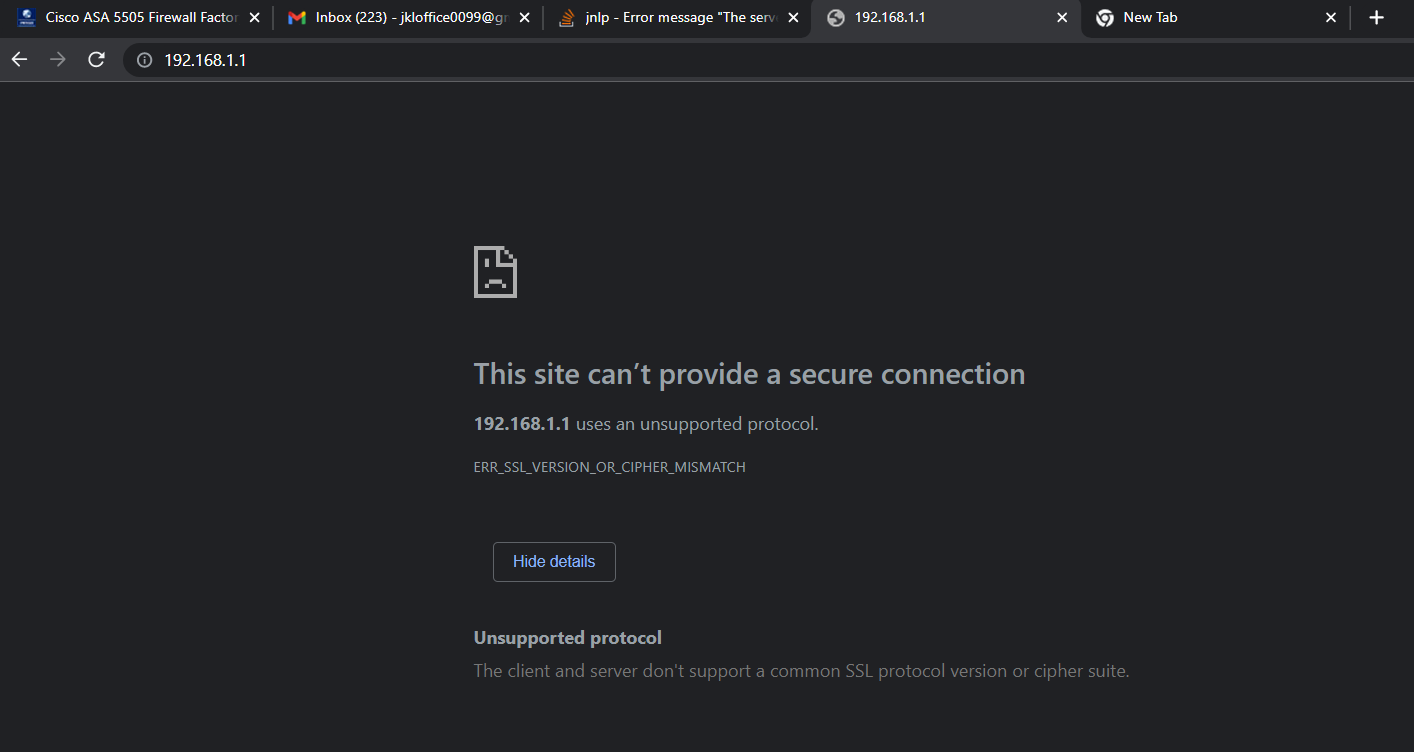
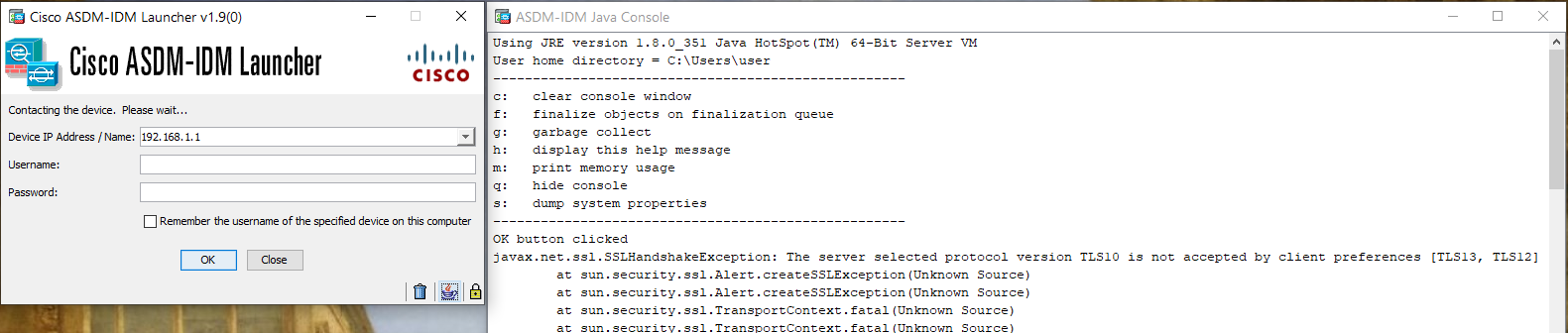
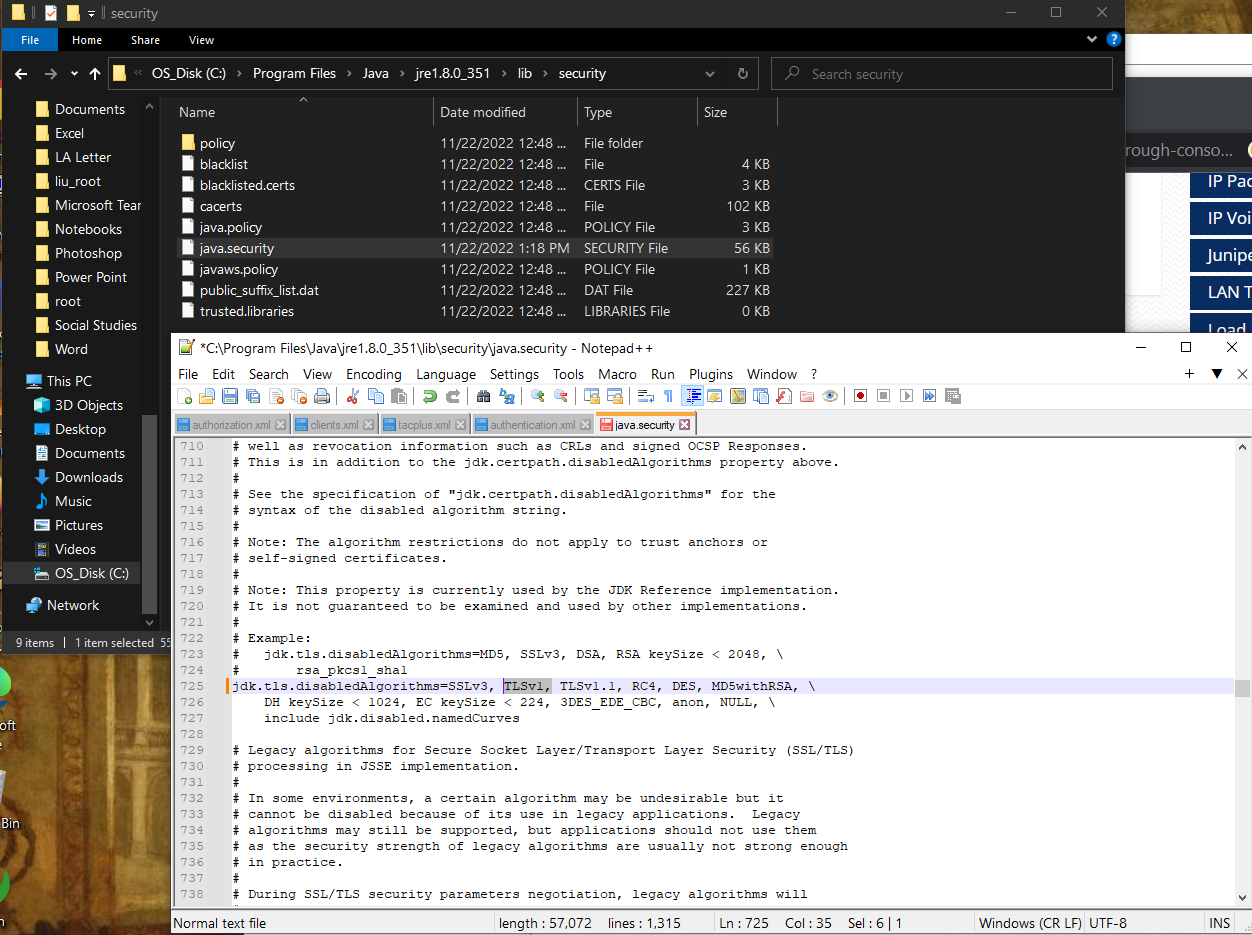
As the lab was incomplete, all recorded troubleshooting efforts are recorded here.

First, upon seeing that the ASDM-IDM launcher desktop icon has appeared after running the execution file, it was to our surprise the shortcut does not work. It simply did not open anything. We learned that this was a common issue, and the shortcut’s file path was inherently incorrect, and not the file that it should have been directed to. Using online guides, such as the YouTube video <https://www.youtube.com/watch?v=yzfgpcnrUbI&ab_channel=EfrenPlaza>, the shortcut properly opened the ASDM initial screen. This is the same screen that the executable .jar file would open to as well.

The error that followed the desktop icon method was that after entering the management IP address, it would not load the ASDM. The initial screen, called the IDM launcher, would disappear and nothing would follow. This issue indicates that file redirection was still an error and not fully fixed.

**** The other method of attempting to access the ASDM was to open the .jar file from Program Files directly. Entering the management IP, we were successful in entering the ASDM launcher. However, it appears like a blank template. As it attempts to the load the configuration from the firewall, the loading bar would get stuck at 17%. After researching possible causes, we learned there were many potential points of error. The first being an incorrect version of Java. For our corresponding ASDM version of 7.12(2), one forum found it successful to change the Java runtime environment version to 7 rather than the newest one of 8. After implementing a different Java version and reloading the firewall, there was no change detected.

Status of loading and displaying current configuration is stuck at 17%. Further configurations cannot be done.

**** Another attempt was to change the Java security file to change the TLS versions. Because, according to the Cisco ASDM-IDM Java Console, TLS version 1.0 was not compatible with the client preference of TLS 1.2 and 1.3. Entering the *java.security* file under the downloaded *java lib* folder, we used Notepad++ to change the client preference to 1.0, and thus adding TLS version 1.0 manually to the file, deleting version 1.2. This makes the client preference 1.0. After reloading the firewall to retest the scenario, there was no change detected.

ASDM-IDM Java Console reporting TLS issue. Says, “the server selected protocol version TLS1.0 is not accepted by client preferences of 1.2 and 1.3.”

Manipulating TLS versions in the java.security folder with Notepad++. Replaced TLS v1.2 with v1.0.

Protocol incompatibility error (unsupported protocol) shown below.

There was also an issue in deleting the ASDM to reinstall all of its contents. When I attempted to delete ASDM, removing all the files relating to its contents within the folder, it did not let me run the executable download file again. It would say that it has already been downloaded. Under *Uninstall Or Remove Programs* in Windows, the application says it still exists, despite having none of the contents of the file that it downloaded remain. This official method of deleting the program resolved this issue. However, redownloading and restarting its contents did not change the 17% error.

To review, the desktop shortcut method led to nothing being opened. In the .jar file, where the ASDM-IDM launcher *could* be opened, the status of “loading the current configuration” was stuck at 17%. No changes in Java, TLS, or rebooting made a difference.

The only proper SOHO-configured 5505 ASA at the lab was done by a group where they had a newer ASA version on their firewall. We hypothesized that the older firewall was not compatible with the ASDM version 7.12(2). We searched up and learned that they do not provide older versions of ASDM launchers online. This seems contradictory as we cannot access the older versions (our versions) to update them to the newest level without accessing the ASDM in the first place.

For future suggestion, we will attempt the same procedure done here on this firewall and configure it in the same way for the newer ASA version firewall. If it succeeds, then it will indicate to us that it is an *ASA version to ASDM launcher* incompatibility issue.

**Conclusion**

This was the first lab where we were unable to obtain the objective. Rather, there were many errors and troubleshooting which became the main challenge in understanding the functionalities of the lab. Ranging from learning about TLS, to Java runtime environments, to the ASDM launcher versions, there are still many elements and solutions to try to get closer to solving this problem.