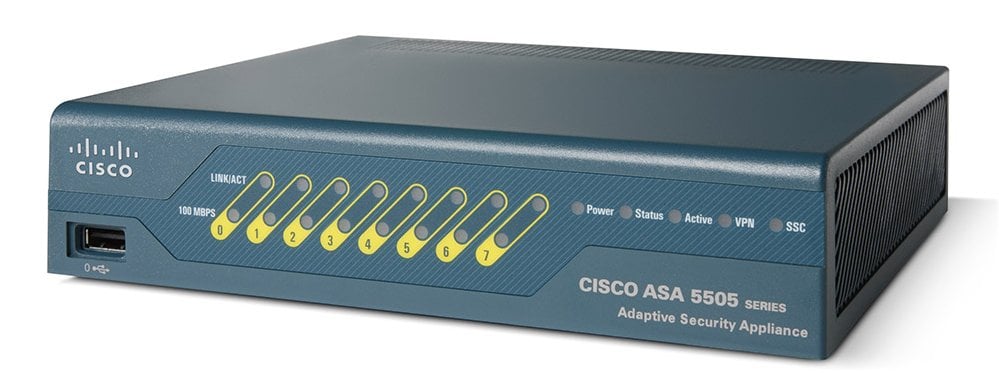
CYBERSECURITY

Sirjan Singh

Cisco ASA Firewall Setup



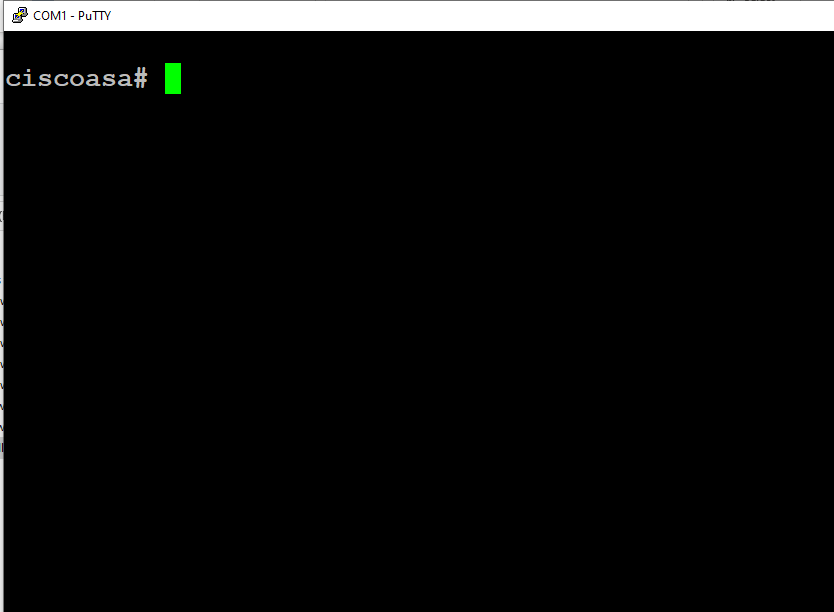
Background: The Cisco ASA is a rather less popular option for firewall when compared to other firewall solutions such as Palo Alto. However, it is still used its capabilities include firewall, antivirus, intrusion prevention, and Virtual Private Network (VPN). Cisco provides a lot of well-organized documentation of the firewall and its new versions which makes it easier to perform functions of the firewall and makes troubleshooting a little easier. Some features of the firewall include access control for the network, application filtering, URL filtering, threat protection, and services for virtual environments. The cisco firewall is renowned in the firewall world for its use of stateful inspection to optimize user experience. An example of stateful inspection improving user experience is when internal users make requests to the internet, an ASA saves session information so that when a valid response comes back, it can recognize and permit the traffic to come back through even packets leave the network as it remembers the valid source and destination IP. Finally, ASAs also have the capability to NAT and PAT capabilities for users, making it convenient.

Our sole purpose of the lab was to get to the UI management of the firewall. One of the biggest disadvantages of the Cisco firewall that we found was that it is not easy to reach the User Interface of the firewall that manages the firewall. In fact, it is so inconvenient that the vast majority of this lab was simply dedicated to simply reach ASDA (Adaptive Security Device Manager). The SOHO configuration was simply a secondary part. Reaching the ASDA requires you to install Java on your machine (not the complicated part), but also requires you to put configuration through the console. In stark contrast, Palo Alto and Pfsense do not require the installment of any additional software and their management interface can immediately be reached by plugging yourself into the firewalls’ management interface, changing your PCs ip address to be in the same network as the management interface, and then typing the management ip on the web. Another unique, but kind of good thing about the cisco firewall is that you can manage the firewall by connecting to any port, instead of having to connect your PC to the management port or connecting your management port to the LAN of your firewall.

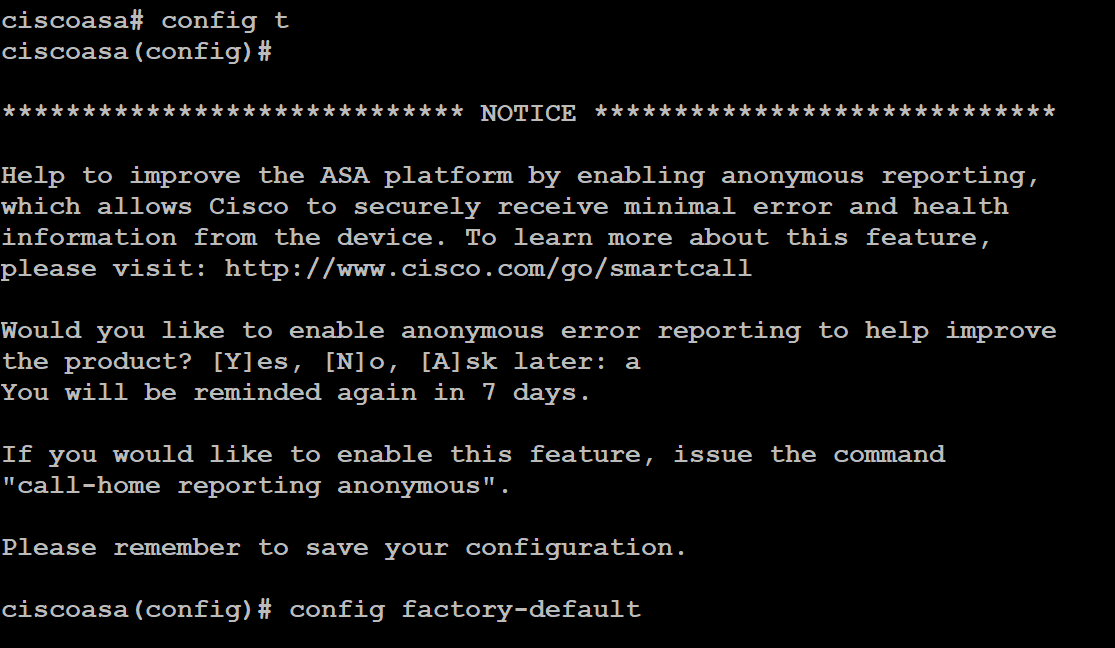
Due to a lack of previous experience with this firewall, we were actually not able to reach the ASDM at all. Whenever we tried to launch the ASDM, we were getting no error, but the screen would be stuck at the 17% mark and stay there. For that reason, we will only be showing step that we did to get to the “stuck at 17%” screen.

Lab Summary

Step 1: After plugging into the console interface, you will get the follow screen.

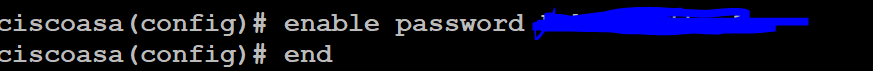


Step 2: Enter configuration terminal and type the following command to configure factory defaults.

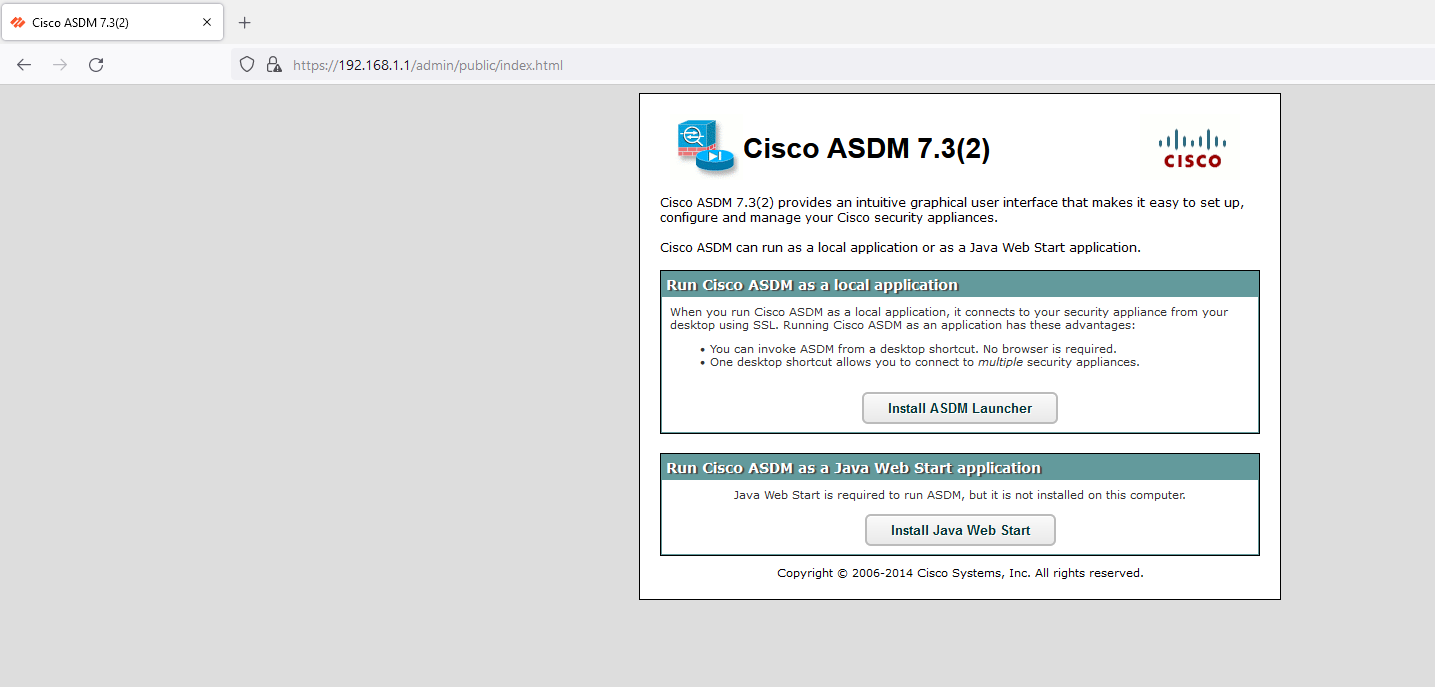


Step 3: reload the firewall after that. 

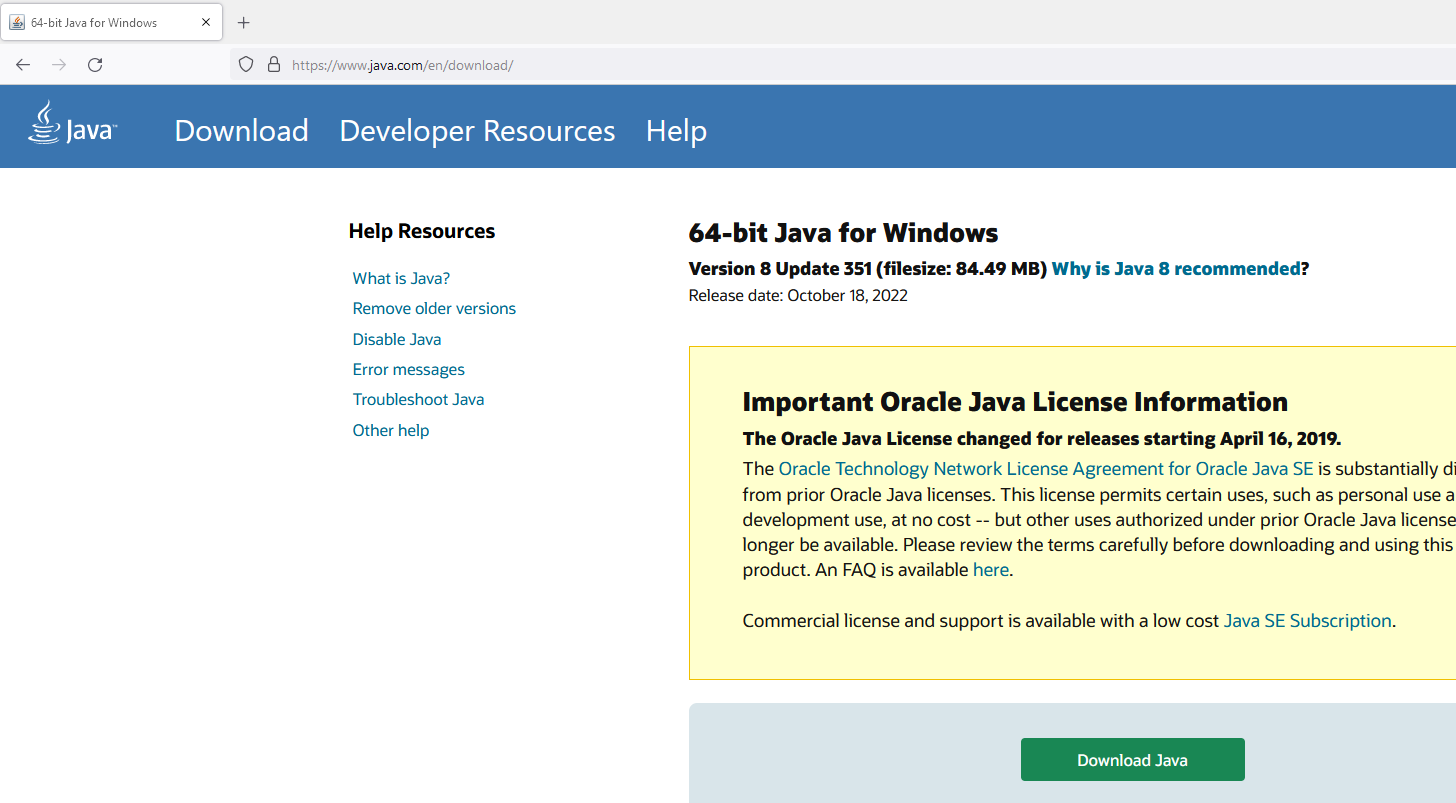
Step 4: create a password on the firewall with the following commands once the router reloads



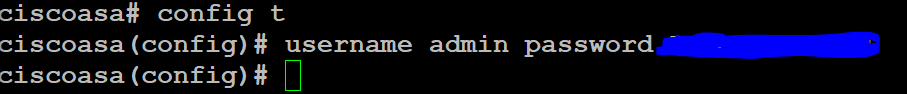
Step 5: Next, connect your PC to any port in the firewall LAN and go to 192.168.1.1 to get to the following page. (You might have to manually configure your PC to be in the same network as the management IP.



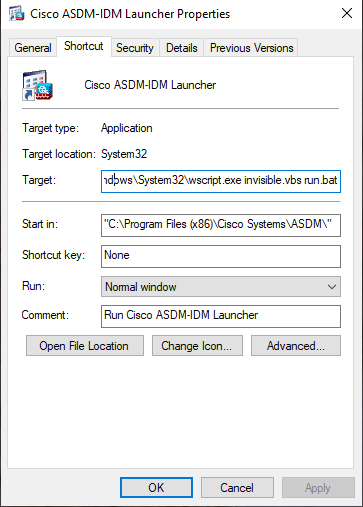
Step 6: Now, install java by going to the following website. For detailed instructions, go to the website and follow the steps there.



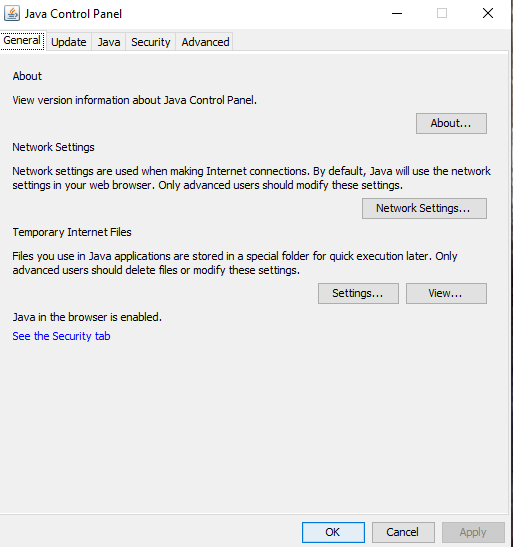
Step 7: Put the following config through the console in your firewall.



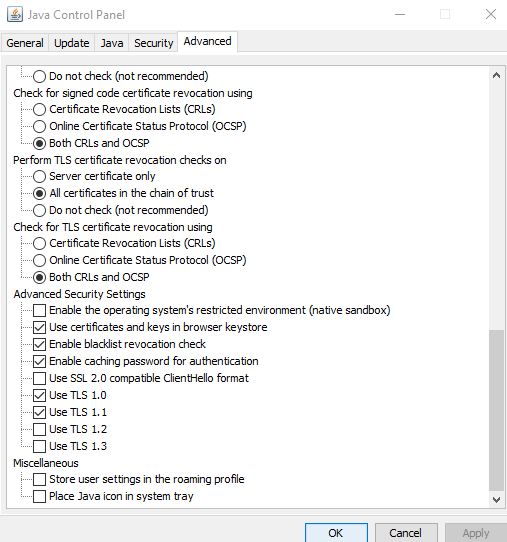
Step 8: When you install ASDM, you will come across the following launcher. Replace whatever the default target is with “C:\Windows\system32\wscript.exe invisible.vbs run.bat”



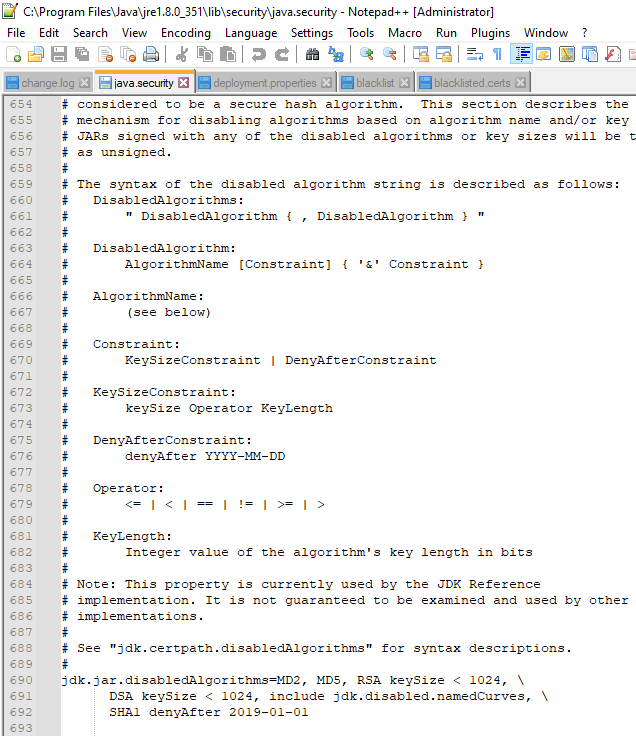
Step 9: When you come across this page, go to advanced



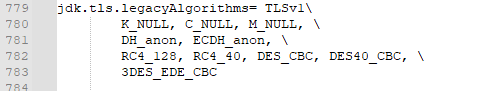
Step 10: Make sure these are the configurations that you have under the advanced tab.



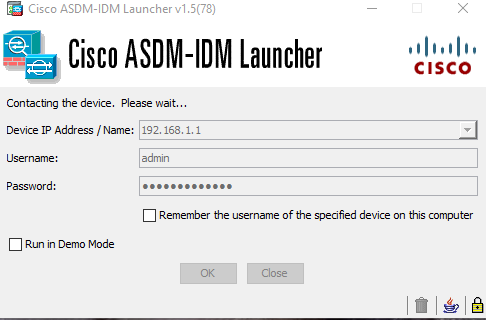
Step 11: Go to the java.security file (location is on the top of the file).



Step 12: Add the following lines to the file



Step 13: Use the step 7 admin and password to login in to the ASDM now



Problems

There were some major problems that we faced during this problem, some of which barred us from completing the initial goal of the lab. First, when we were launching the Cisco ASDM, we were unsuccessful. We realized that we might need to change the location to which our app was launching. So, we changed the default location to which the app was launching the location specified in step 9. We also realized that the java.security file needed to be modified as a requirement for even the launcher to work because a certain protocol required to launch ASDM was blocked in the security. After this, we were at least able to open the ASDM.

This should’ve been the end of the lab, however once the launcher was opened, a message that said “loading configurations” started to load a bar which reached 17% and got stuck there. After changing some other optional settings in the java.security files and rebooting our firewall several times, every time we launched the ASDM, it got stuck at 17%. Frustrated, we searched this specific problem on the internet and realized that this was a very, very common problem for Cisco ASA users. One of the most common solutions recommended on online forums for this problem was to factory reset the whole cisco ASA, do steps 1-9 again and then load the config back per tftp in the running config. As this was a common solution, we were hopeful it would work but it did not, and instead our firewall started running into some other problems such as its lights taking unusually long to load. For that reason, we simply left the firewall alone for a few minutes and removed the tftp config. We then cross checked every single config that we put on the firewall with another group (the only group whose thing worked) and we still did not find the issue.

Conclusion

This lab, though not conclusive in the way we wanted, forced us to use a lot of troubleshooting techniques as well as perform actions that we normally would never have applied to access the user interface of a firewall. For example, we went in a Java file and tried to put configurations. Though in the end we weren’t successful, we know now for the future that this is a potential source of error because fixing the java.security file worked for some of our other peers. We continue to try different things such as putting the same configurations on another cisco firewall (to see if out piece is just faulty). This is an unlikely case since this appears to be the problem that many, many face and are unable to find the solution to on tech forums. In the end, though we weren’t that concerned about the cisco firewall anyway as it is inferior to other firewall, we still tried to set it up to diversify the number of firewalls we have experience with. In that sense, we kind of were successful.