**Cisco firewall factory reset**

Derek Liu Cybersecurity Period 5

Lab #6

**Restoring Cisco ASA to Factory Default***Derek Liu*

Purpose

The purpose of this lab is to become familiar with the Cisco ASA and figure out how to factory reset the device and access the web interface.

Background Information

When accessing a Cisco ASA, it is unsure whether or not there were previous configurations on the device. If the intention is to use the ASA in a different network, it usually will be simpler to factory reset the ASA and configure it accordingly for the new network. In this lab, we connect a second-hand Cisco ASA to a network, factory reset it, and then accessed the Cisco Adaptive Security Device Manager (ASDM) launcher -- a web-based graphical user interface -- in order to proceed with configuration for our network.

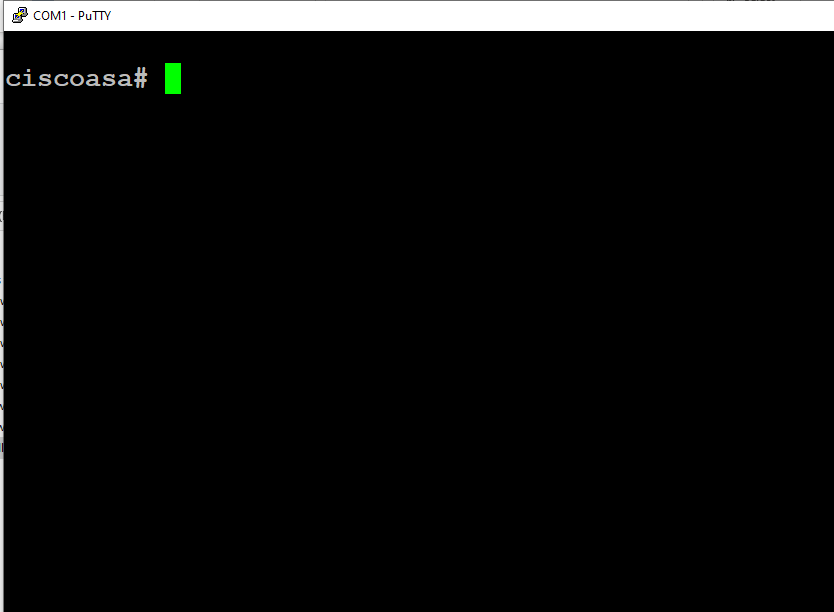
The Cisco Adaptive Security Appliance (ASA) is a security device that provides firewall and network security for various network architectures. It can be deployed as a standalone device or integrated into a larger network. The Cisco ASA is designed to provide multiple security functions in a single device, including firewall, antivirus, intrusion prevention, virtual private network (VPN), and advanced threat protection. It also supports a variety of networking protocols and can be configured to meet the specific needs of an organization. One of the main features of the Cisco ASA is its firewall, which is designed to protect a network from external threats such as hackers and malware. It does this by inspecting incoming and outgoing traffic and allowing or blocking it based on predefined security rules.

This lab was considered completed when the firewall had been successfully integrated into the network. After successfully accessing the ASDM, we found it already was pre-configured for a SOHO environment.

Configurations

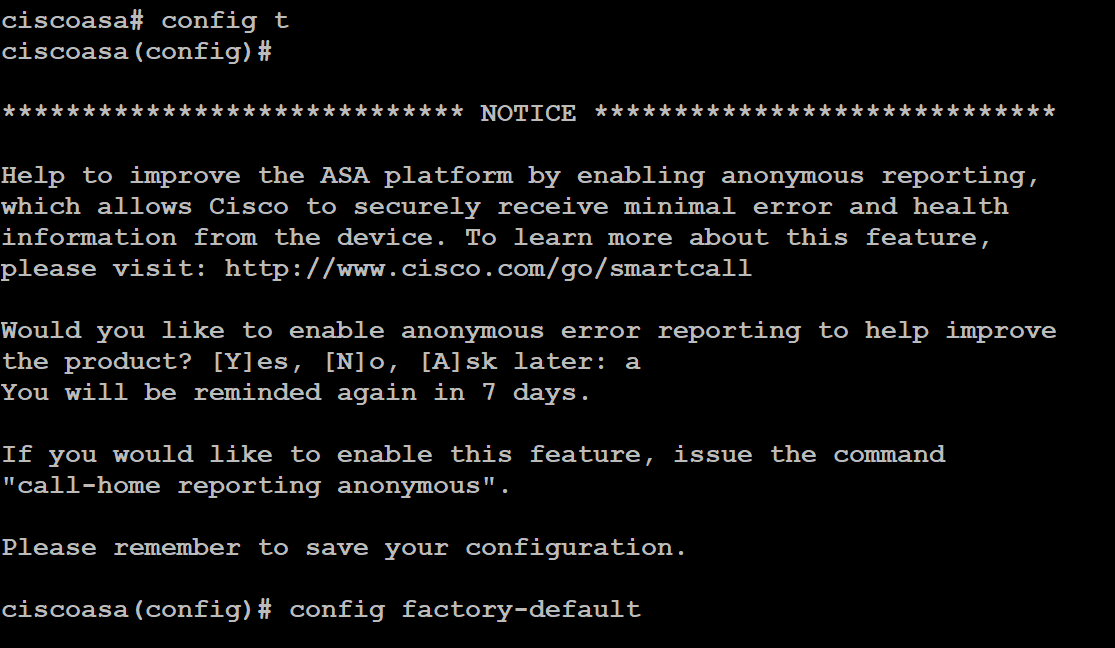
Step 1.

Connect ethernet cable from port 0 of the ASA to the WAN. Connect ethernet cable from any port other than 0 to workstation. Connect console cord into the console port of the ASA. Press the reset button the firewall. Open the terminal on the workstation and type “en”



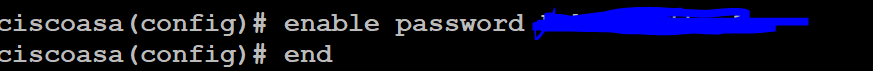
Step 2.

Type “config t” and then “config factory-default”.



Step 3.

Set a password with “enable password [password]”



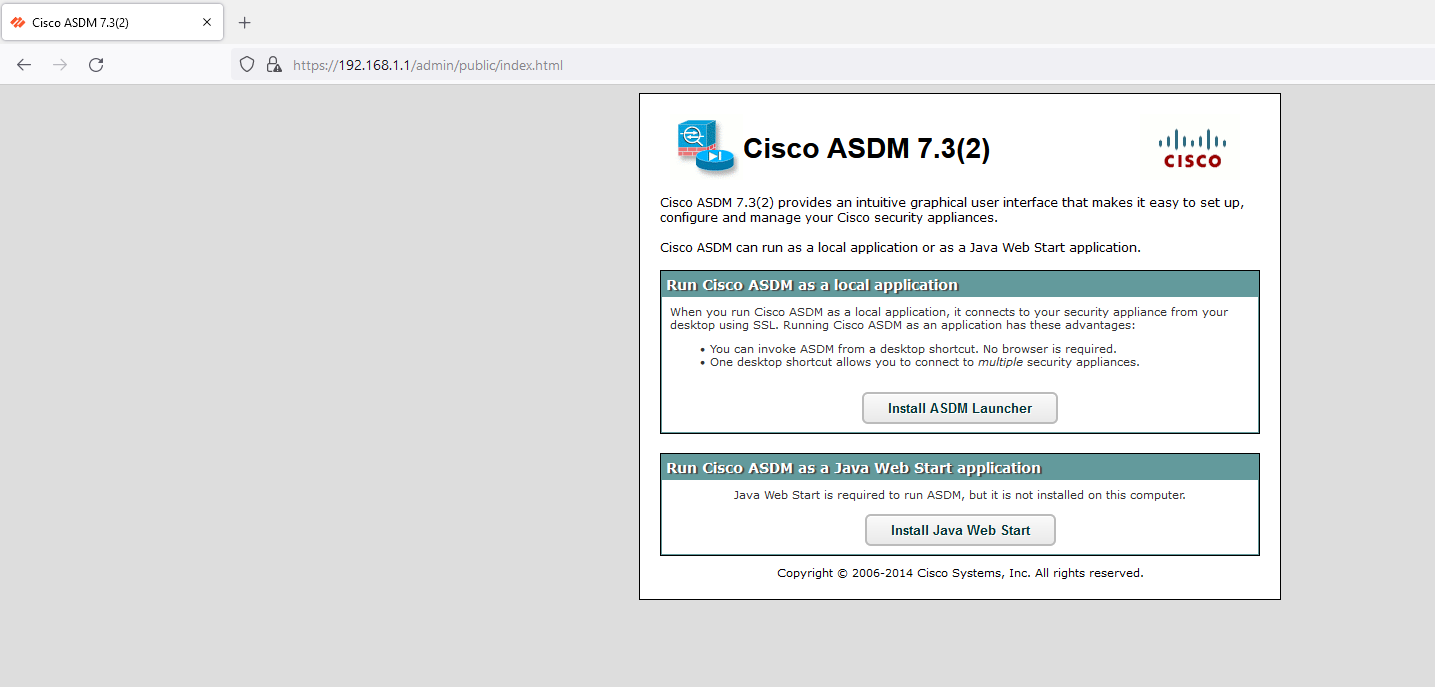
Step 4.

Save the configuration by typing “reload” and saving changes.



Step 5.

The default management address for the ASA should be <https://192.168.1.1/admin>

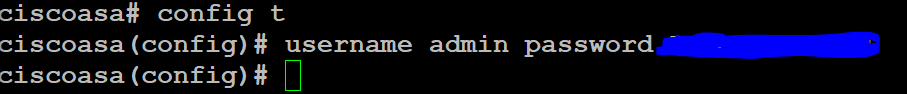


Step 6.

Install Java Web Start on the workstation by clicking “install Java Web start” and install the ASDM launcher by clicking “Install ASDM Launcher”.

Step 7.

Configure a username and password on the CiscoASA (these will be the credentials used to log into the ASDM launcher).

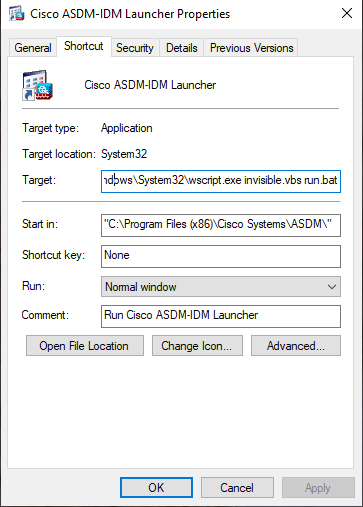


Step 8.

On the workstation’s desktop, there should be an installed desktop shortcut. Right click the icon and select “properties”

Paste the following into the target textbox:

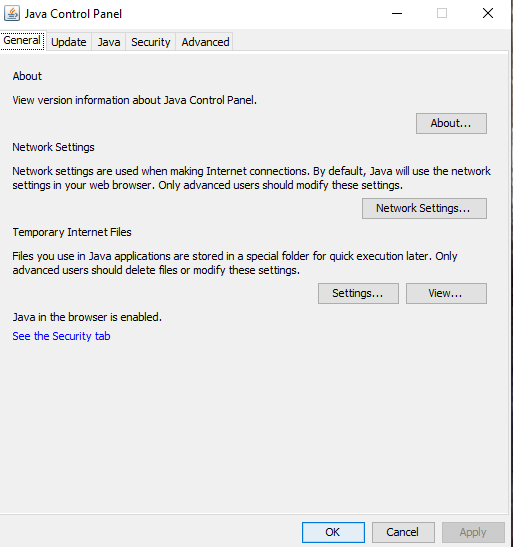
C:\Windows\system32\wscript.exe invisible.vbs run.bat



Step 9.

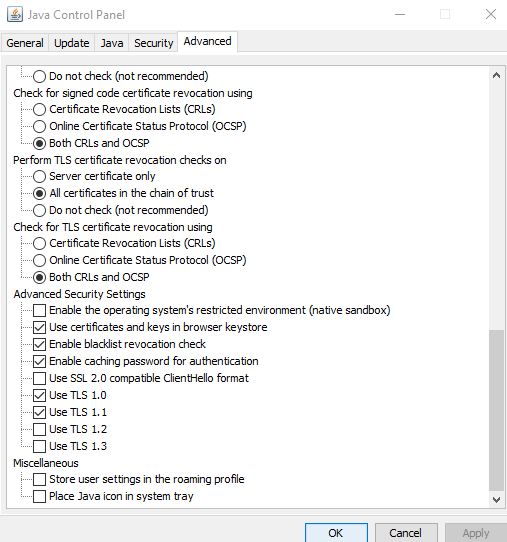
Open the workstation’s control panel (windows + r and search “control”).

Select “Programs” and then “Java.”



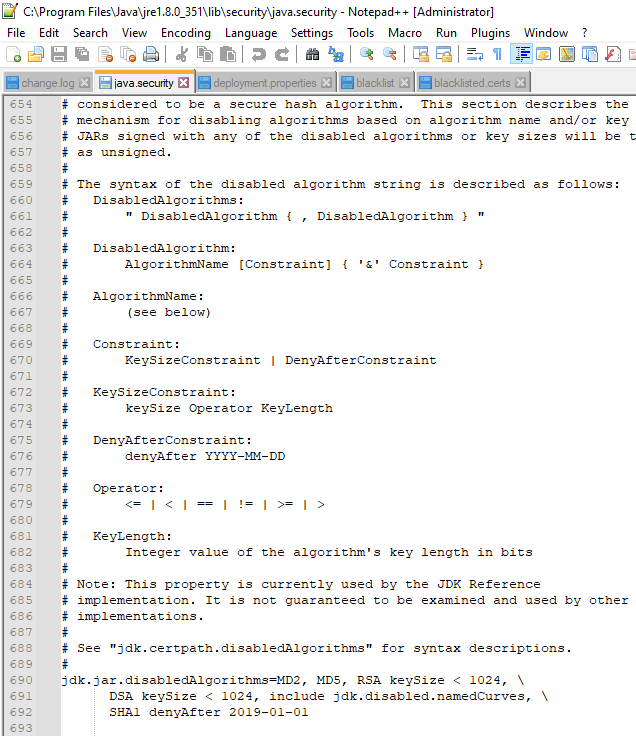
Step 10.

Go to “advanced” and scroll down. Enable only TLS 1 and TLS 1.1



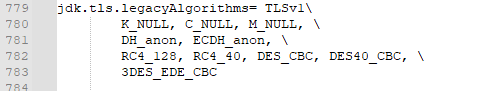
Step 11.

Open the file explorer on the workstation and go to C:\Program Files\Java\jre1.8.0\_351\lib\security\java.security



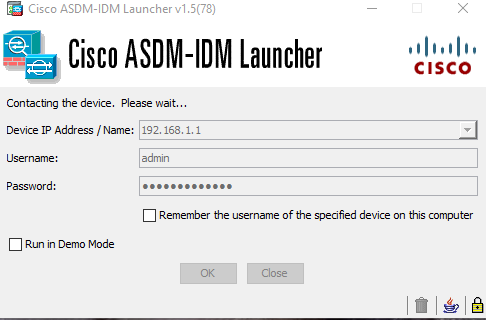
Step 12.

Under jdk.jar.disabledAlgorithms, remove TLSv1 and TLSv1.1 and under jdk.tls.legacyAlgorithms add TLSv1. Save the file.



Step 13.

Open the ASDM launcher and type in the IP address of the ASA. Use the username and password configured in step 7.



Problems

A problem that we ran into while setting up the ASA was the connection on the web interface failing initially but that started working after the ASA received an IP address from the WAN side and enabled TLS on the workstation. Most problems arose from trying to use the Cisco ASDM Launcher. Starting with trying to use the desktop shortcut, initially it wouldn’t open. This was fixed by editing the properties of the launcher and changing the target application in shown in step 8 of the configuration. After and trying to enter the device IP and credentials, an error message appeared on the Java console that said that the TLS version being used is not compatible with the system preferences of TLSv1.2. Our solution to this was to lower the preferred TLS version. This was done by removing TLSv1.1 and TLSv1 from disabled algorithms in the Java program files and changing the settings of settings of Java to use TLS 1.0 and TLS 1.1.

Conclusion

In this lab, we obtained a used a used Cisco ASA. We used a workstation with a console cord to console into the firewall to enter restore it to factory defaults. After factory resetting the ASA, we installed the required files to access the Cisco ASDM Launcher. After changing program preferences and program files due to an abundance of error messages that we had to work around while trying to access to Launcher, we were ablet to access the configuration GUI. We can use this GUI to configure the ASA for our network in the future.