

Cisco Firewall 5505 Factory Reset

Evan Choi | Cisco Cybersecurity | 1/31/2023**Purpose**

The purpose of this lab is to factory reset a Cisco ASA 5505 firewall so we can use it to setup a Small Office Home Office (SOHO) configuration. It should be accessible through the Adaptive Security Device Manager (ASDM) and its Java environment.

**Background Information on lab concepts**

The Cisco Adaptive Security Appliances (ASA) 5505 firewall was released as part of the Cisco ASA 5500 Series in May 2005, and succeeded the following three lines of Cisco products, all popular in their own respect: Cisco PIX, Cisco’s IPS 4200 Series, and Cisco VPN 3000 Series Concentrators. Cisco ASA has also become one of the most popularly used firewall/VPN solutions for small to medium businesses.

The Cisco ASA 5500 Series ASA integrate world-class firewall, SSL and IPsec VPN, Unified Communications security, intrusion prevention (IPS), and content security services in one product family. This series provides intelligent threat defense and secure communications services that protect businesses from attacks. They allow organizations to lower their overall operations and deployment costs while delivering multilayer security.

The Cisco ASA 5505 specifically, is the smallest device, with it’s compact 8 port design. These 8 ports feature 10/100 Fast Ethernet switches which can be dynamically grouped to create up to three different VLANs for home, business, and Internet traffic. It also provides two Power over Ethernet (PoE) ports. You can configure it with the Adaptive Security Device Manager (ASDM). You must download the ASDM launcher software from the ASA firewall, which can be done by entering https://<ASA-Address>/admin in your browser.

**Lab Summary**

Although this lab is incomplete, all steps done so will be documented and recorded.

We first consoled into the firewall using PuTTY, and factory reset the firewall using the “config factory-default” and “reload save-config noconfirm” commands. Then, we changed the PC address so it was in the same subnet as the management IP address, and entered that IP address into an internet browser, which led us to the download page, where we downloaded the java runtime environment and ASDM launcher.

After entering the management address into the screen on the ASDM, the loading bar to access the configurations would get stuck at 17%. After researching online, it was visible that the number 17% appeared for many other people. We could not find a working solution, and therefore our progress stopped. Since we couldn’t access the ASDM, we couldn’t configure the firewall.

**Lab Commands**

The following commands were used in the Cisco CLI.

show version – Checks the version of the firewall

enable – Enters enabled mode

configuration terminal – Enter global configuration mode

config factory-default – Resets the firewalls configuration settings to factory settings

reload save-config noconfirm – Reloads/reboots the firewall

**Procedure**

1. Console into the Cisco CLI using PuTTY. Use the Lab Commands, as shown in the image and lab commands section

Text

Description automatically generatedText

Description automatically generated

1. Access the management IP address using an internet browser. We used **Firefox.** Click the blue, **Enable TLS 1.0 and 1.1** button to go to the page.

A screenshot of a computer

Description automatically generated

1. The ASDM page should appear now

Graphical user interface, text, application

Description automatically generated

1. Now, download the **ASDM Launcher.**

Graphical user interface, text, application, chat or text message

Description automatically generated

1. Java is required for this, click the **Java Web Start** button. It should bring you to the Java Runtime Environment Download website.

Graphical user interface, text, application, email

Description automatically generated

1. Now, download **Java version 8u351** for Windows x64.

Graphical user interface, text, application, Word

Description automatically generated

1. Java should now successfully download.

Graphical user interface, text, application, email

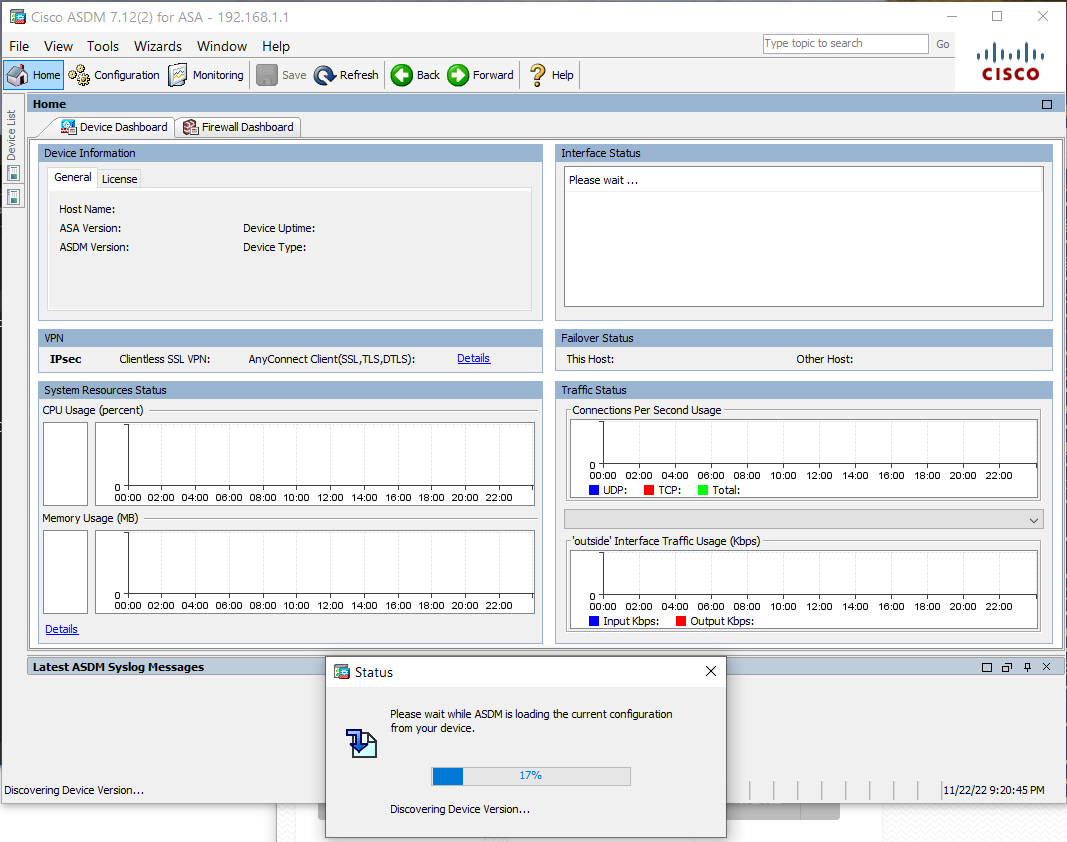
Description automatically generated

1. Open the **asdm-launcher.jar** file. Enter the device IP.

A screenshot of a computer

Description automatically generated

1. Once you enter the default device IP, the ASDM will appear.



1. In the image above, you will notice that the status bar is stuck at 17%. This is the point where we got stuck and couldn’t progress further in the lab.

**Problems**

With the lab being incomplete, all our troubleshooting attempts will be documented here.

First, after downloading the ASDM-IDM launcher, we saw a desktop icon appear, but after running it, it didn’t work. We figured out that this issue was common, and that the shortcut was incorrect.

An issue that happened following the opening of the desktop shortcut, was that after entering the management IP, the ASDM would not load. There would be a screen called the IDM launcher that would periodically appear, then disappear. We learned that this indicated that the file redirection had an error.

Another thing we attempted was going into the Java security file to change the TLS versions. We did this because after researching, we found that TLS version 1.0 is not compatible with TLS 1.2 and 1.3. After entering the **java.security** file in the **java lib** folder, we used Notepadd++ to change the client preference to 1.0, and added TLS 1.0 manually into the file, and deleted TLS version 1.2. According to the website we used, this would make the client preference 1.0 and it would work. After saving the file, we reloaded the firewall, but no change got detected.

A picture containing text

Description automatically generated

The above message says “the server selected protocol version TLS 1.0 is not accepted by client preferences of 1.2 and 1.3” so we made 1.0 the client preference

Graphical user interface, text, application

Description automatically generated

In the above image, we changed the TLS versions in the java.security folder.

The last issue we ran into was when deleting the ASDM to reinstall everything. When we tried deleting the ASDM, it wouldn’t let us run the executable download file. A message would appear saying that the file was already downloaded, and when checking Uninstall Or Remove Programs in Windows, it would say that it still exists, although we had uninstalled everything relating to that file.

When doing this lab, we did it with other groups of people, and out of all the groups, only one had succeeded. We realized that their firewalls version was newer than ours, so we concluded that our older firewall wasn’t compatible with the ASDM version.

**Conclusion**

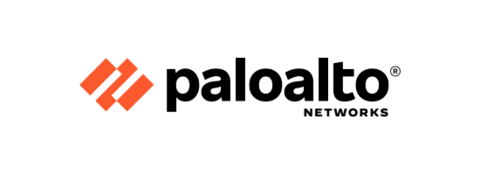
In this lab, we were unable to achieve our desired objective. We ran into many errors and issues in this lab, and although we attempted to troubleshoot them in a variety of different ways, we couldn’t find a working solution.

The stamp below recognizes that

Evan Choi

has completed

**Lab 6 – Cisco Firewall 5505**

 Adv Cisco Cybersecurity – Mr. Mason & Mr. Hansen

Period 5