Cisco ASA

By: Jordan Abu-Zahra

**Purpose**

In this lab we set up a Cisco ASA so that it could run in a SOHO configuration and work and provide internet to our network.

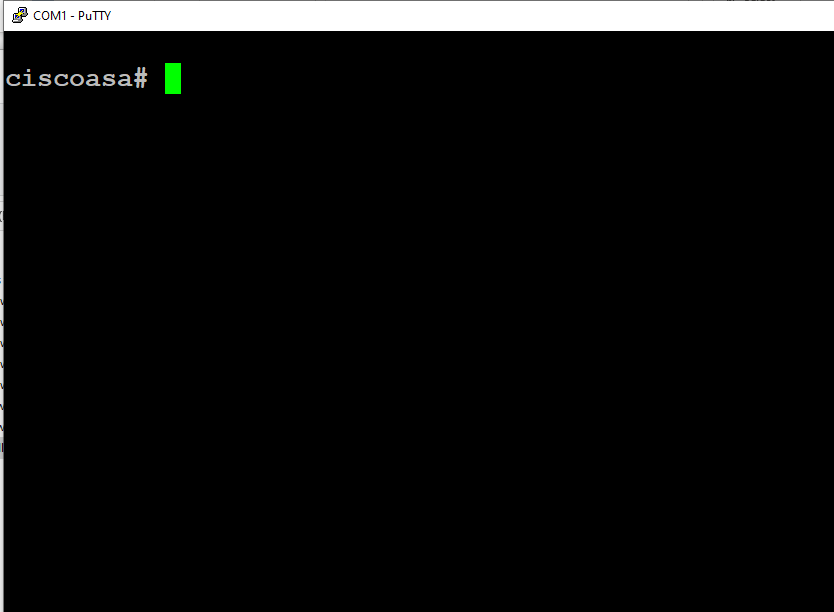
**Background**

Cisco ASA (Adaptive Security Appliance) is a security device from Cisco Systems that combines firewall, antivirus, intrusion prevention, and VPN capabilities in a single device. It is designed to provide network security from a small to medium sized business and enterprise level organizations, the Cisco ASA firewall provides stateful and deep packet inspection for all network traffic, including both IPV4 and IPV6. It can also be configured to provide VPN services, including remote access, VPA, Site-to-site VPN, and SSL VPN. The firewall can also provide protection against intrusion and malware using intrusion prevention systems and antivirus features. Some features the Cisco ASA’s provides is Access control list which allow the user to define and add security policies by controlling access to network resources, VPN’s which allow connect remote users or sites to the corporate network, NAT which allows internet access for the internal uses and it hides the internal IP address, content security to protect against malware and other unwanted traffic, and high availability to increase system availability and reduce downtime, and the firewall is also often integrated with other cisco security solutions such as cisco Identity services engine for network access and cisco firepower for advanced threat protection. Cisco ASA’s are available in different models and sizes to meet the desired requirement, such as the number of users, throughput and number of interfaces. In our previous lab we used Palo Alto firewalls and the difference is that Palo Alto could base and is more suited for modern, cloud-based environments while the ASA is more traditional and may be better fit for organizations with more of a legacy infrastructure

**Steps**

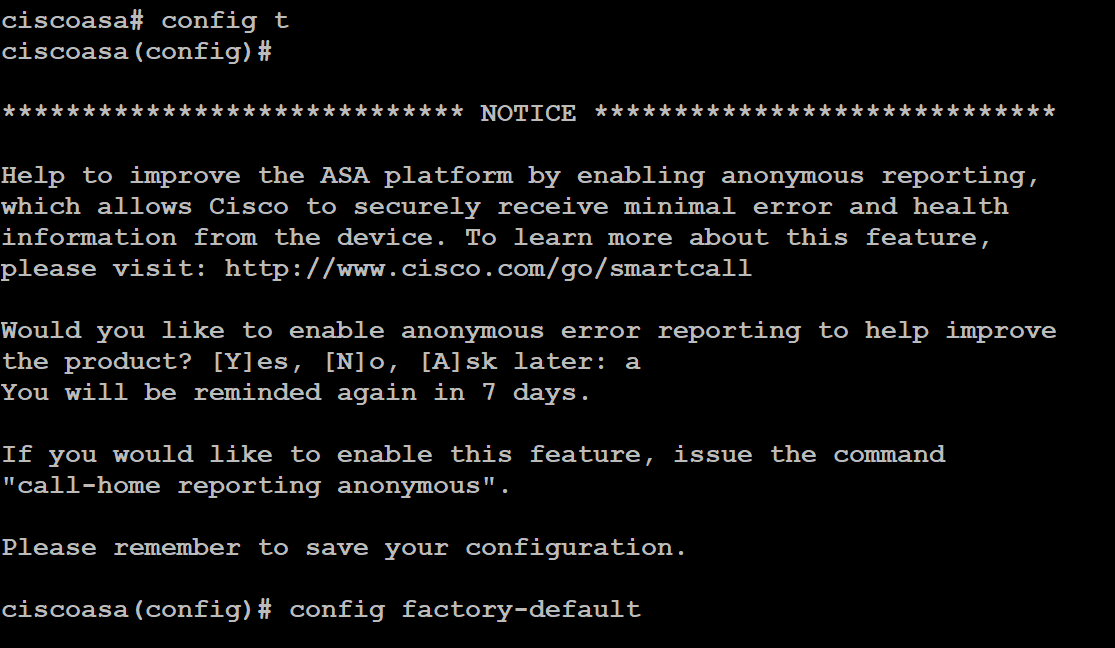
Step 1.

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”



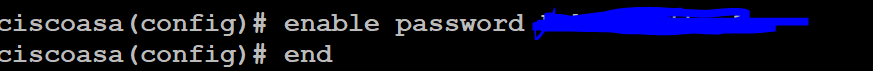
Step 2.

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



Step 3.

Set a password with “enable password [password]”



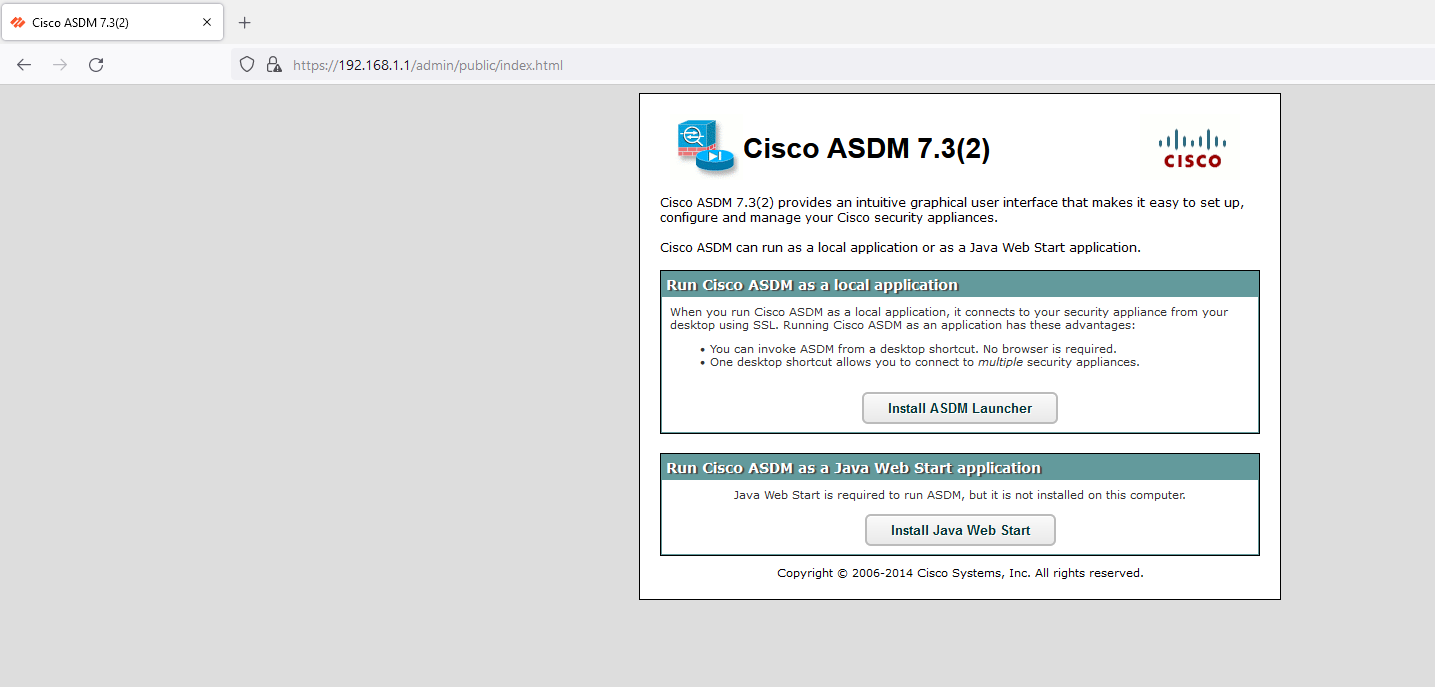
Step 4.

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>

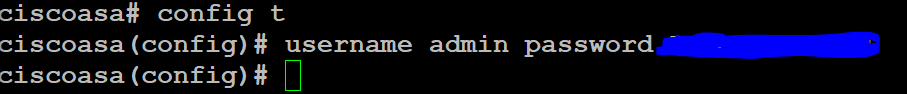


Step 6.

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).

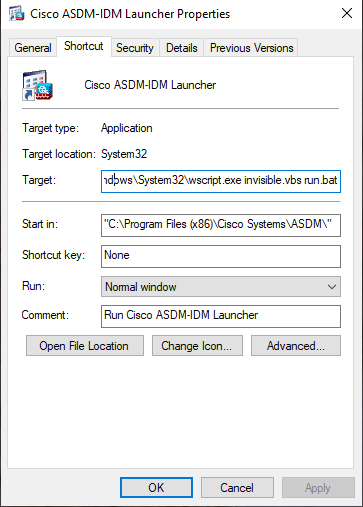


Step 8.

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:

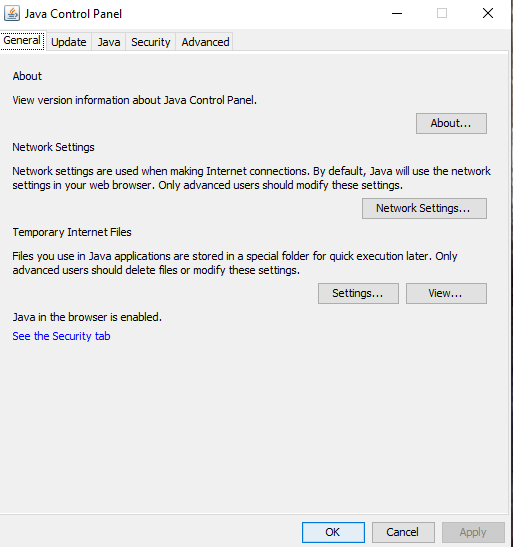
C:\Windows\system32\wscript.exe invisible.vbs run.bat



Step 9.

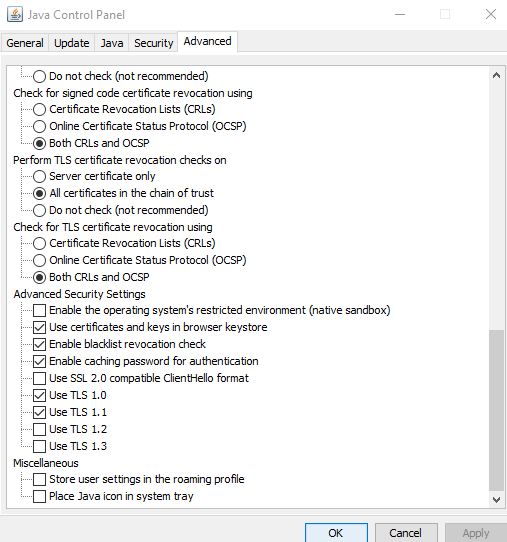
Open the workstation’s control panel (windows + r and search “control”).

Select “Programs” and then “Java.”



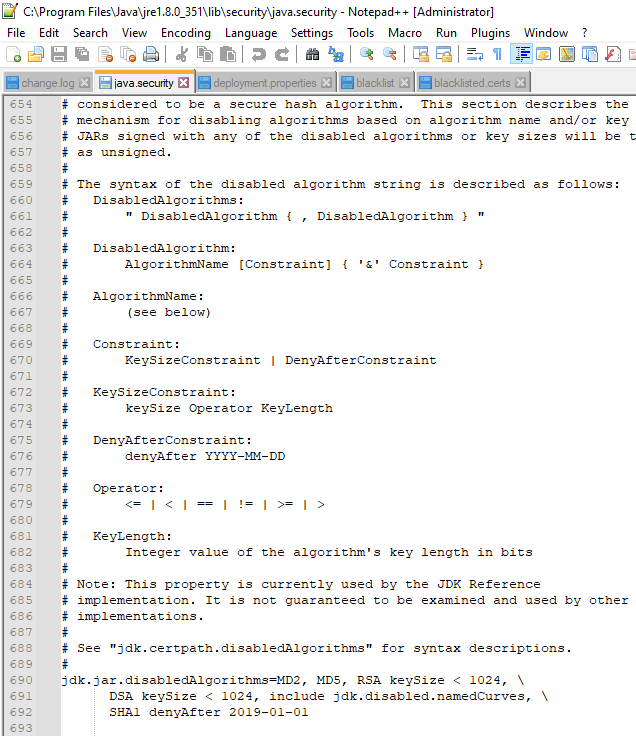
Step 10.

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



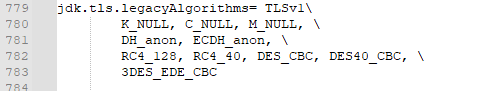
Step 11.

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



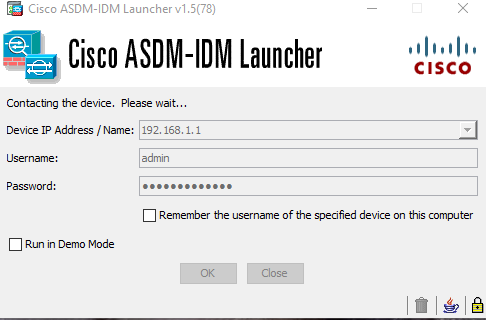
Step 12.

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**

In this lab we face a small number of problems but one of them was getting into the web interface, we had to change the properties of the application and had to change the target application. Another problem we faced was that we had to wrong version of TLs and had to go into the java file telling us to allow this type of TLS and remove it from the file so it could use the outdated version of TLS.

**Conclusion**

In conclusion we learned how to set up a CISCO ASA and learn a bit of java on the side.