

Cisco ASA 5505 Firewall Lab Configurations

Sophia Zhang | Period 5 Cybersecurity | 2022-2023



**Purpose:**

The purpose of this lab was to perform a factory reset on a Cisco ASA 5505 and get into the launcher.

**Background:**

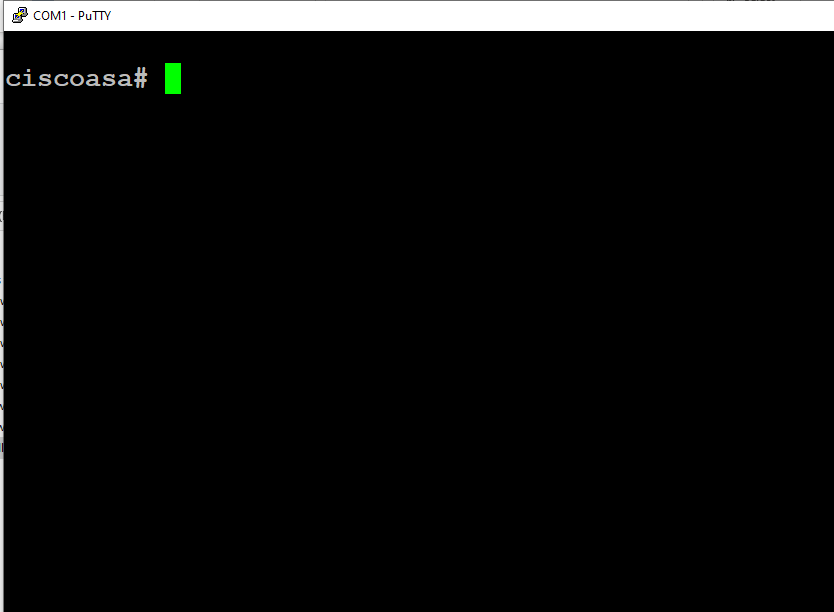
Cisco ASA firewall is a sort of outdated firewall. Cisco uses two different OS. It is normally used for small offices or branches. What we do for our lab is to factory reset it and access the launcher. The issue is that the launcher wouldn’t load for us, and we think it has to do with Java version however we are not completely sure. The lab is technically incomplete, but we are to do a write up with what we have.

The ASA has PoE and uses Cisco ASDM Adaptive Security Appliance. On the firewall you can use it for SOHO and DHCP. ASA stands for Adaptive Security Appliances. The ASA series started being released in 2005. It has become one of the most common firewalls in the industry. There are a lot of complaints with the GUI however. There has also been existence of flaws. The software is based on Linux. Like other cisco devices it has Rommon and configuration does need to be done on the actual firewall.

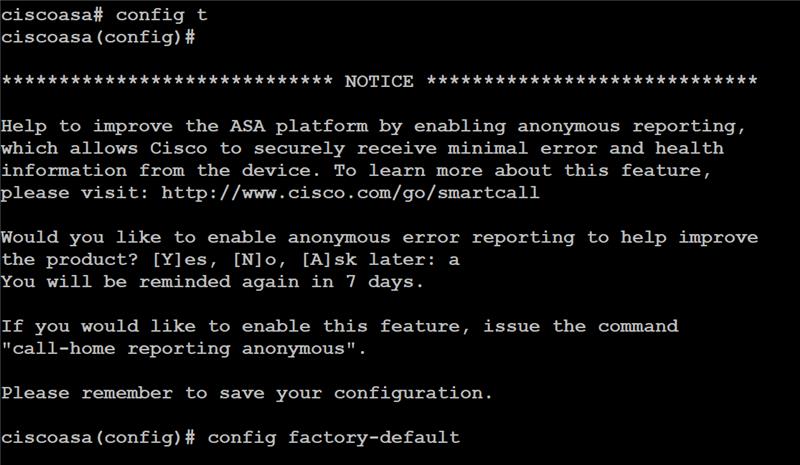
For the lab we do need to access Rommon in order to factory reset and this is also called Maintenance mode. Maint mode is accessed by using a break key. As of 2018, the firewall models run on 64-bit processing instead of 32. These models start at the 5506, the firewalls we have come before then. The 5505 succeeded the CISCO PIX, CISCO IPS 4200, and the CISCO VPN 3000. The software on the firewall is very similar to Cisco IOS which is found on Cisco routers which makes it very familiar as we have used it many times before. ASDM which the ASA uses stands for Adaptive Security Device Manager. It lets you manage the ASA through a local web interface. In other words, it gets you to a GUI to configure the Firewall through the web.

**Lab Procedure:**

1. Open Putty



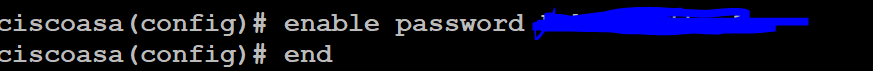
1. Enter global configuration mode by typing “config t” and press enter, and type “config factory-default” and press enter.



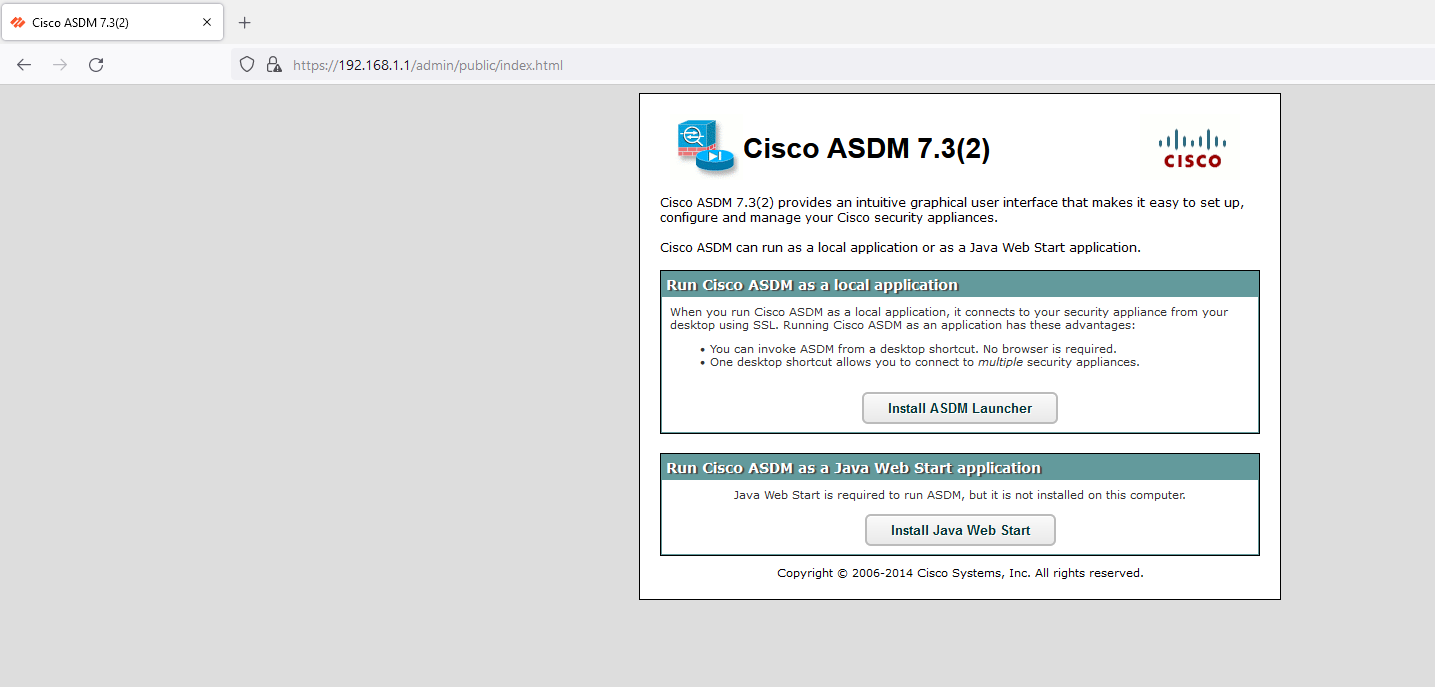
1. Exit global configuration mode and type “reload”. When asked if you want to save, enter “y”.



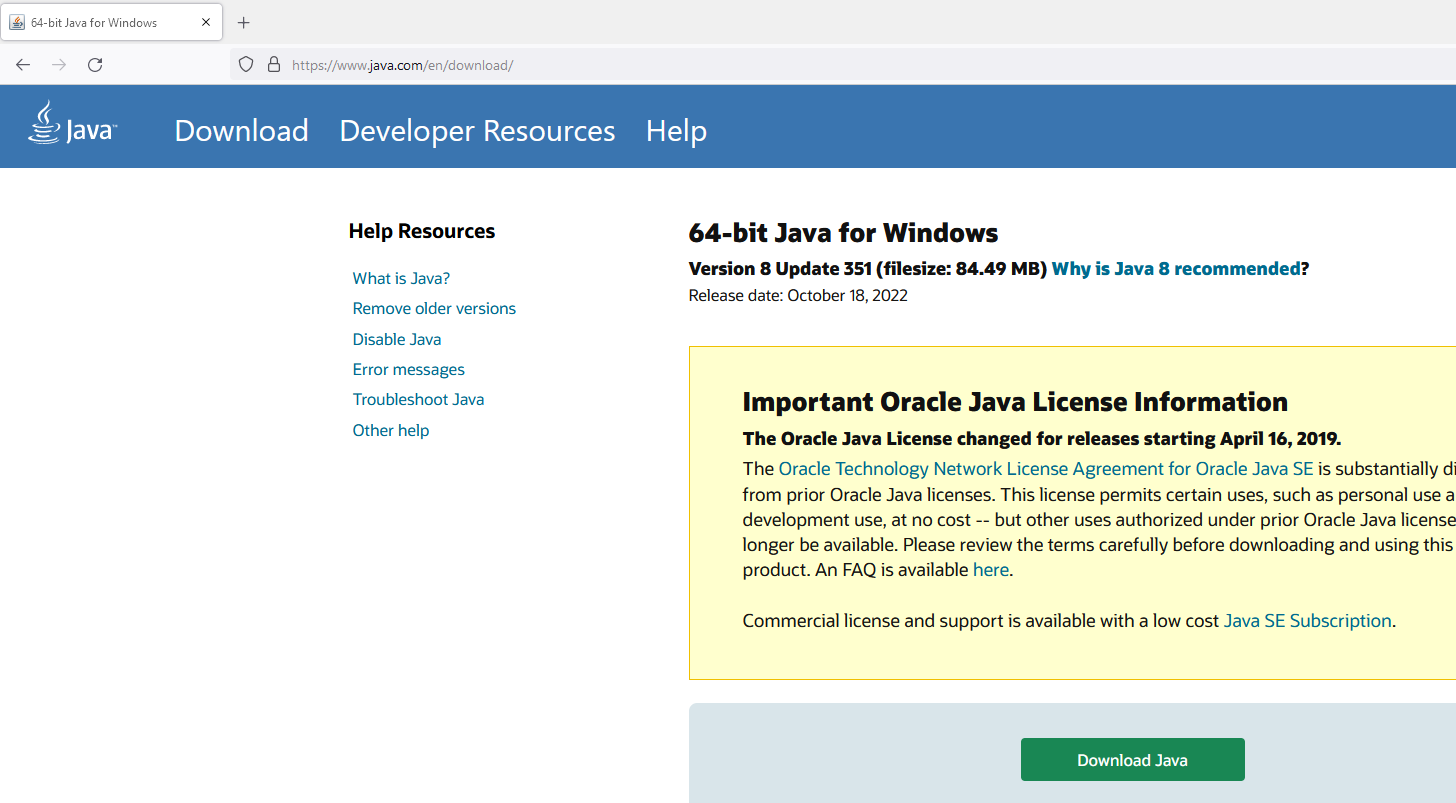
1. Type “config t” and press enter. Set a password by typing “enable password” and then your desired password. Then, type “end”.



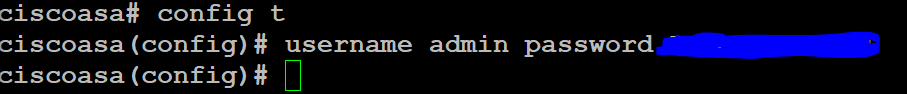
1. Go to Firefox, and enter “<https://192.168.1.1/admin/public/index.html>” into the search engine.



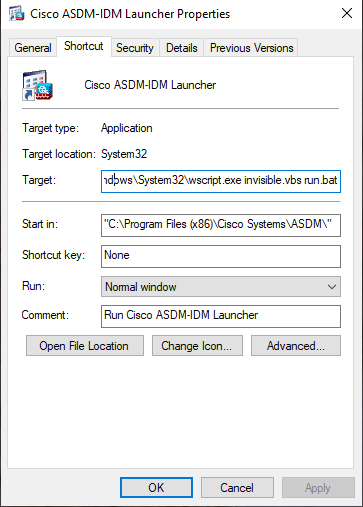
1. Click “Install Java Web Start”



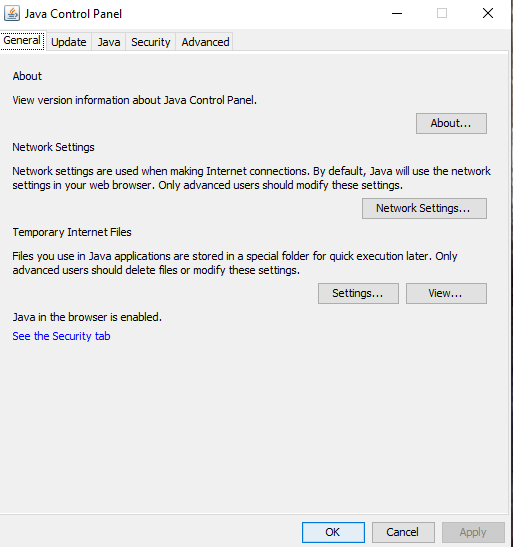
1. Return to Putty and set another password by entering global configuration mode and entering “username admin password” and your desired password.



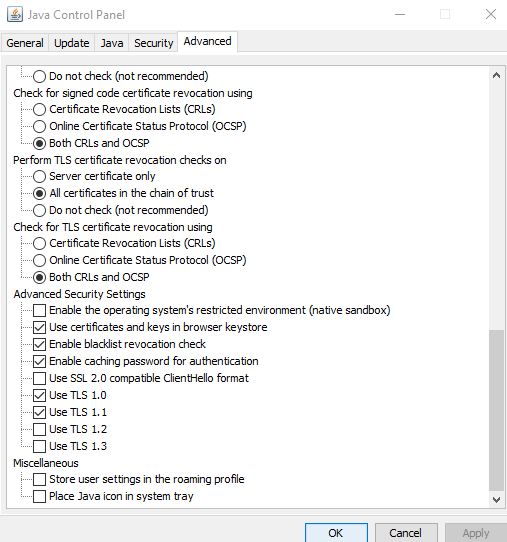
1. Enter Cisco ASDM-IDM Launcher Properties, and type “C:\Windows\system32\wscript.exe invisible.vbs run.bat” into Target, and configure as shown below:

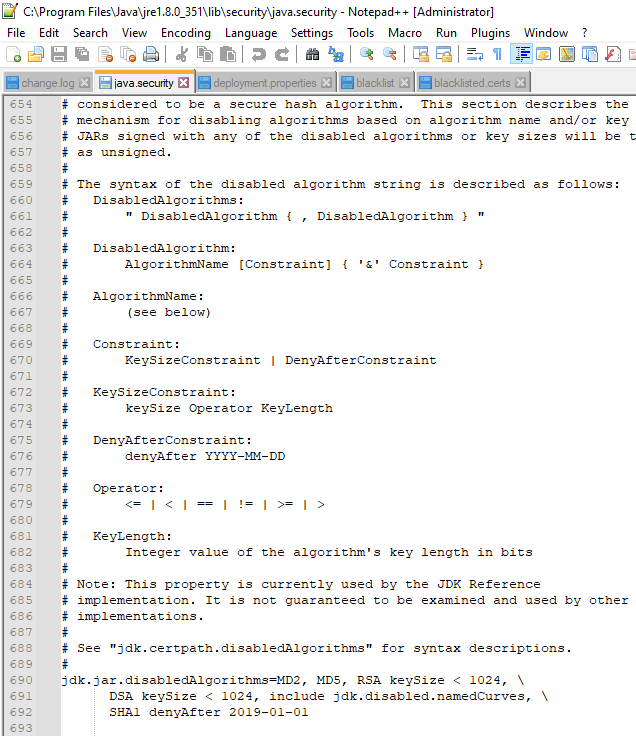


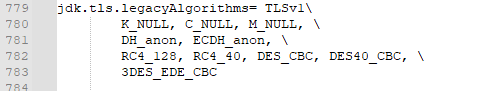
1. Enter the Java Control Panel:



1. Enter the Advanced tab, and configure as shown below:







1. Go to Cisco ASDM-IDM Launcher v1.5(78) and enter your username and password as configured previously:



**Configurations:**

hostname ciscoasa  
enable password 7hjtQYKNE/v7sd6z encrypted  
names  
!  
interface Ethernet0/0  
switchport access vlan 2  
!  
interface Ethernet0/1  
!  
interface Ethernet0/2  
!  
interface Ethernet0/3  
!  
interface Ethernet0/4  
!  
interface Ethernet0/5  
!  
interface Ethernet0/6  
!  
interface Ethernet0/7  
!  
interface Vlan1  
nameif inside  
security-level 100  
ip address 192.168.1.1 255.255.255.0  
!  
interface Vlan2  
nameif outside  
security-level 0  
ip address dhcp setroute  
!  
ftp mode passive  
object network obj\_any  
subnet 0.0.0.0 0.0.0.0  
pager lines 24  
logging asdm informational  
mtu inside 1500  
mtu outside 1500  
icmp unreachable rate-limit 1 burst-size 1  
no asdm history enable  
arp timeout 14400  
no arp permit-nonconnected  
!  
object network obj\_any  
nat (inside,outside) dynamic interface  
timeout xlate 3:00:00  
timeout pat-xlate 0:00:30  
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02  
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00  
timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00  
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute  
timeout tcp-proxy-reassembly 0:01:00  
timeout floating-conn 0:00:00  
dynamic-access-policy-record DfltAccessPolicy  
user-identity default-domain LOCAL  
http server enable  
http 192.168.1.0 255.255.255.0 inside  
no snmp-server location  
no snmp-server contact  
crypto ipsec security-association pmtu-aging infinite  
crypto ca trustpool policy  
telnet timeout 5  
no ssh stricthostkeycheck  
ssh timeout 5  
ssh key-exchange group dh-group1-sha1  
console timeout 0

dhcpd auto\_config outside  
!  
dhcpd address 192.168.1.5-192.168.1.132 inside  
dhcpd enable inside  
!  
threat-detection basic-threat  
threat-detection statistics access-list  
no threat-detection statistics tcp-intercept  
username admin password GGI7m.ypAgeTxiwJ encrypted  
!  
class-map inspection\_default  
match default-inspection-traffic  
!  
!  
policy-map type inspect dns preset\_dns\_map  
parameters  
  message-length maximum client auto  
  message-length maximum 512  
policy-map global\_policy  
class inspection\_default  
  inspect dns preset\_dns\_map  
  inspect ftp  
  inspect h323 h225  
  inspect h323 ras  
  inspect rsh  
  inspect rtsp  
  inspect esmtp  
  inspect sqlnet  
  inspect skinny  
  inspect sunrpc  
  inspect xdmcp  
  inspect sip  
  inspect netbios  
  inspect tftp  
  inspect ip-options  
!  
service-policy global\_policy global  
prompt hostname context  
call-home reporting anonymous prompt 1  
Cryptochecksum:8588cfc69a440683bd936c14add93730  
: end

**Problems:**

Our main issue in this lab was that we were unable to finish the lab fully. The loading stopped at a percentage, and never finished loading. Also, our group was required to learn specific configurations that would only be used for this lab. We had to search for java files, and we were unable to find out the reason why some worked, and why the others were unsuccessful. Lastly, the steps weren’t clear, so we were left to figuring the lab out on our own.

**Conclusion:**

In this lab, we performed a factory reset on a Cisco ASA 5505 and got into the launcher.