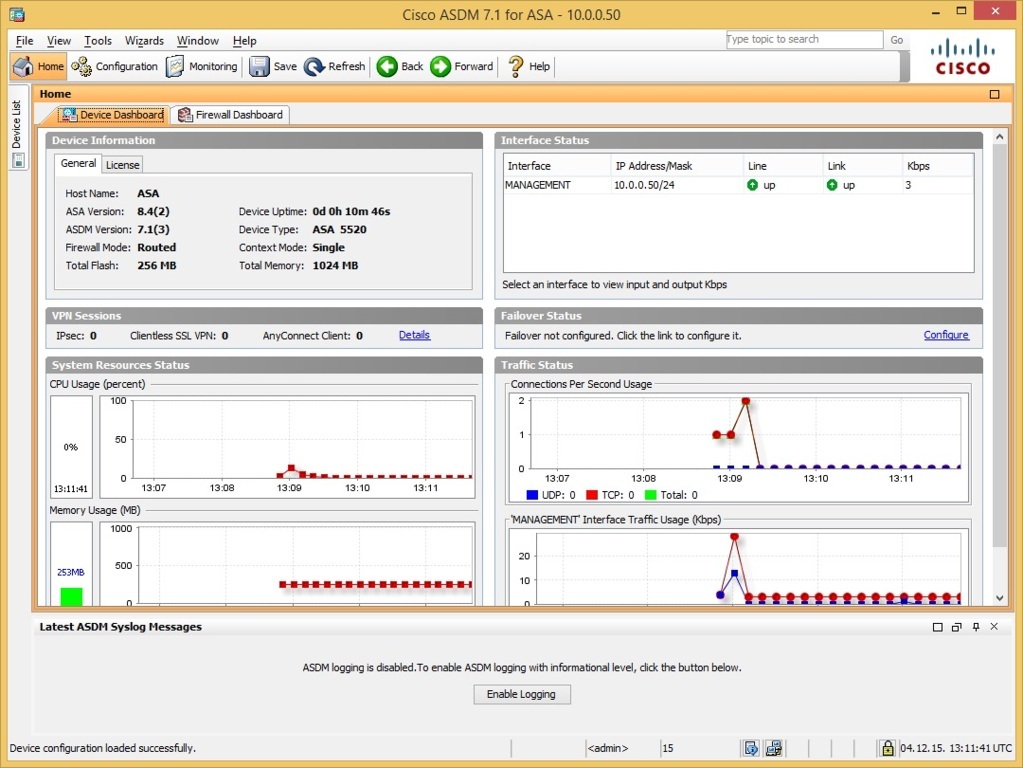
Setup of ASDM GUI



**Purpose;** This lesson focused on setting up and utilizing the ASDM GUI.

**Background information on lab;** Cisco's Adaptive Security Device Manager (ASDM) is the GUI tool used to manage the Cisco ASA security appliances. The Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. It provides proactive threat defense that stops attacks before they spread through the network.

**Lab Summary;** In this lab, we figured out how to set up the ASDM GUI which enables us to manage Cisco ASA appliances. This management allows us to manage, firewall, antivirus and virtual private networks remotely. To enable this, we started out with entering a few commands into the command line. These commands included setting up IP addresses for each individual VLAN, creating two different interfaces, outside and inside interfaces with differing security levels for both interfaces. We enabled the outside interface as a DHCP client, and the Century link router is acting as our DHCP server. These commands allow us to reach the internet on our management laptop where we then enter the ip address of our inside interface to reach the ASDM download link. We download the asdm from the link open the ASDM type the password and username we set up for the ASA and enter into the ASDM. Now we have full access to management of the ASA and have several helpful tools for configuring the ASA.

**Commands**

: Serial Number: JMX1237Z0B8

: Hardware:   ASA5505, 1024 MB RAM, CPU Geode 500 MHz

:

ASA Version 9.2(4)14

!

hostname ciscoasa

enable password 8Ry2YjIyt7RRXU24 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 192.168.10.1 255.255.255.0

!

interface Vlan2

 nameif outside

 security-level 0

 ip address dhcp setroute

!

ftp mode passive

object network INSIDE\_SUBNET

 subnet 192.168.10.0 255.255.255.0

object-group icmp-type ALLOW\_ICMP

 icmp-object echo-reply

 icmp-object time-exceeded

 icmp-object unreachable

 icmp-object traceroute

access-list INBOUND extended permit icmp any any object-group ALLOW\_ICMP

pager lines 24

logging asdm informational

mtu inside 1500

mtu outside 1500

icmp unreachable rate-limit 1 burst-size 1

asdm image disk0:/asdm-751.bin

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

!

object network INSIDE\_SUBNET

 nat (inside,outside) dynamic interface

access-group INBOUND in interface outside

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 0.0.0.0 0.0.0.0 inside

http 0.0.0.0 0.0.0.0 outside

no snmp-server location

no snmp-server contact

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpool policy

telnet 0.0.0.0 0.0.0.0 inside

telnet 0.0.0.0 0.0.0.0 outside

telnet timeout 5

no ssh stricthostkeycheck

ssh 0.0.0.0 0.0.0.0 inside

ssh 0.0.0.0 0.0.0.0 outside

ssh timeout 5

ssh key-exchange group dh-group1-sha1

console timeout 0

dhcpd auto\_config outside

!

dhcpd address 192.168.10.100-192.168.10.110 inside

dhcpd dns 4.2.2.2 interface inside

dhcpd enable inside

!

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

!

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

!

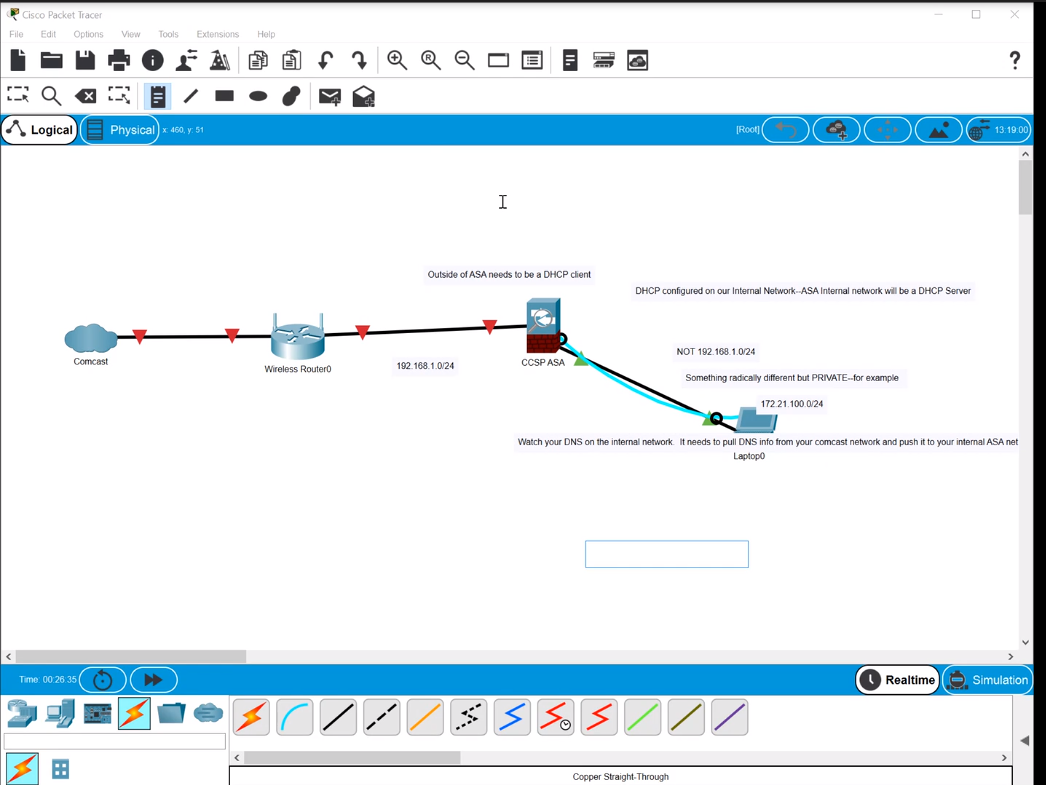
service-policy global\_policy global

prompt hostname context

no call-home reporting anonymous

Cryptochecksum:5109f74174315dc5e1f3e7dfbc4bbb58

: end



**Problems;** We had a variety of issues with this lab. Primarily, the shortcut for ASDM had the wrong target file location, we changed that to the correct file location and fixed was able to open the application. Secondly configuring a DHCP client on the outside interface was difficult in finding the correct commands but once we found the commands everything worked quite well.

**Conclusion;** In this lab we were able to enable management of the ASDM GUI. In doing so we will be able to manage the ASA along with its firewall, antivirus and VPN capabilities. This will allow us to configure the ASA more effectively in the future. This management will allow us to remotely create and maintain the network.