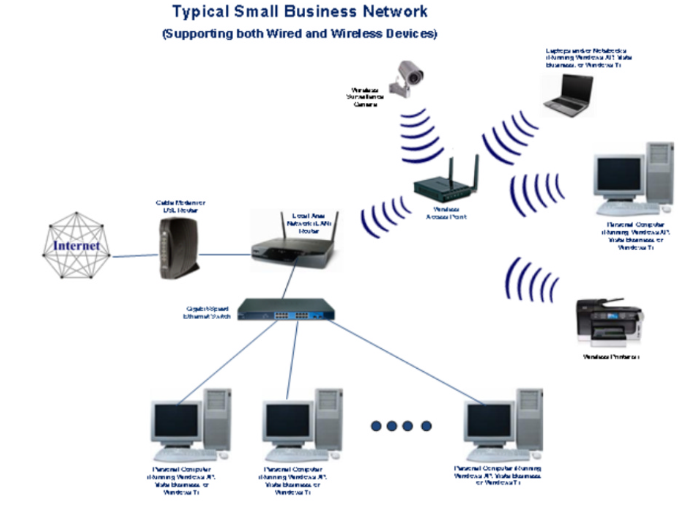
ASA Firewall Configuration for Small and Medium Businesses



**Purpose;** The purpose of this lesson is to configure an ASA firewall for use by small and medium businesses

**Background information on lab**; Cisco`s ASA firewall is a security device that provides protection along with firewall and antivirus capabilities. Losing data to a hacker can be detrimental to any business and especially so to small and medium sized businesses. By utilizing a Cisco ASA firewall and configuring this firewall successfully you can prohibit any malicious actors from stealing or extorting your small business for its valuable information. The firewall is the one item in your network that will fight every outside attack trying to get into your small businesses network.

**Lab Summary;** In this lab, we configured the ASA firewall specifically for Small business and medium sized businesses. We did this through setting up a DHCP and DNS to be able to successfully access the internet outside of our network without allowing any threat actors into our network. This was achieved by routing the DNS traffic in and out of our network with a dynamically set DNS network. This dynamically set DNS server is superior to a statically set DNS server because if there is ever a lapse in connection to your internet providers router DNS will be down and need to be refreshed with the same DNS server address while the dynamically set DNS server will not miss a beat when receiving a new address for the server. This gives around the clock protection the internal network of your business and allows for constant access. In configuring the outside interface as a DHCP client you are enabling a DHCP address to be given to that interface which permits the client to reach the internet outside the network. Additionally, the ASDM GUI allows us to configure the firewall with ease with a variety of different setup and configuration Wizards. In conjunction these configurations allow us to protect a small business network with an ASA firewall.

**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 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

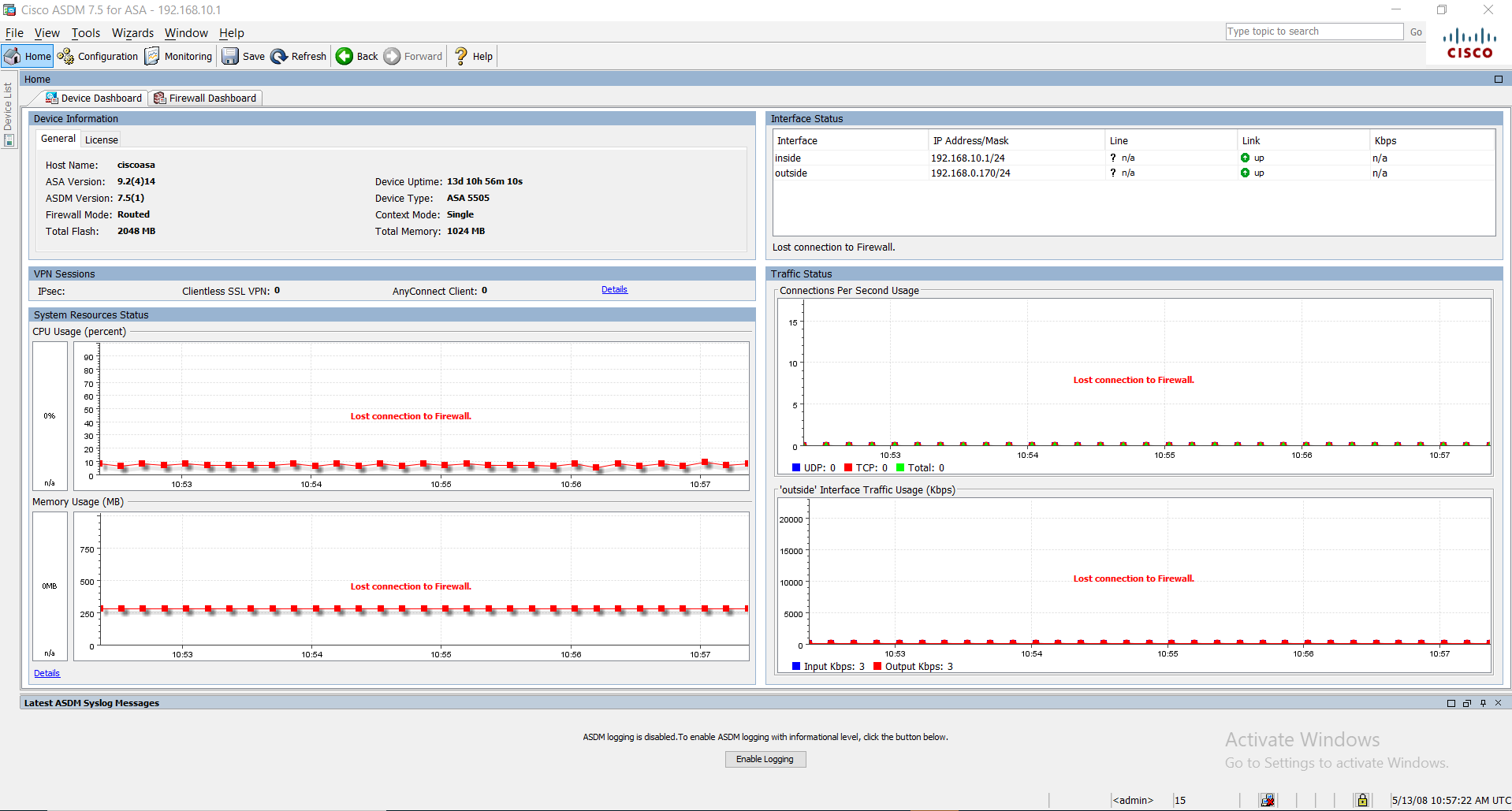
!

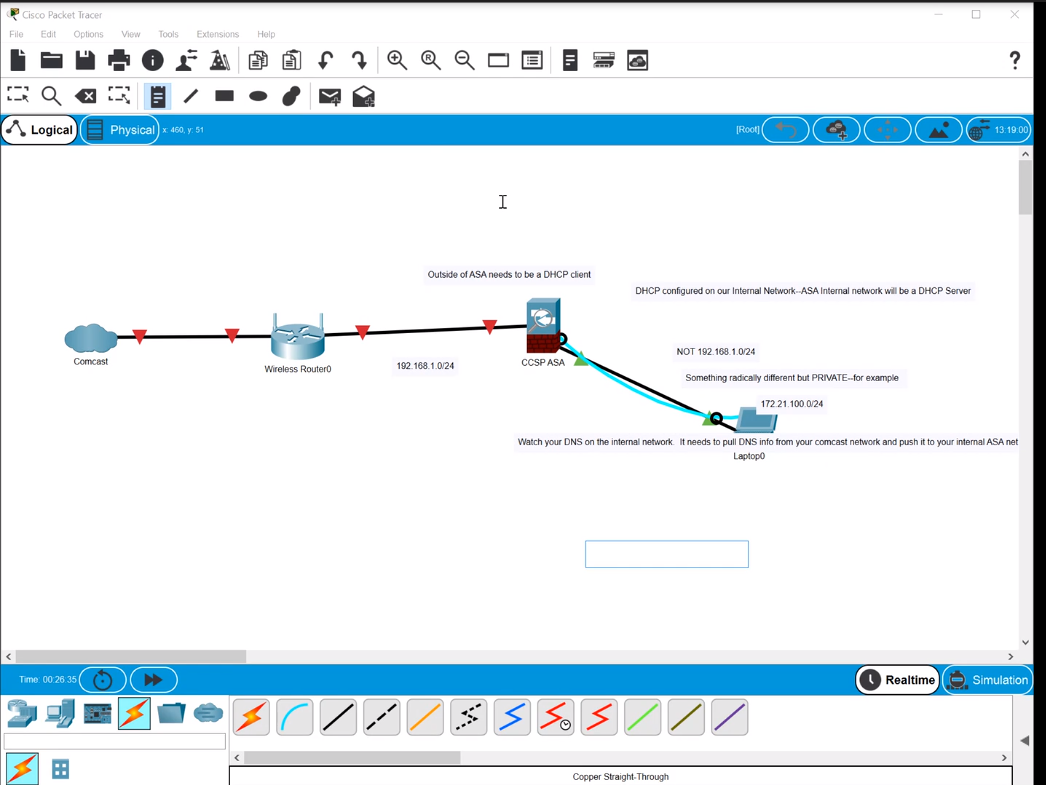
service-policy global\_policy global

prompt hostname context

no call-home reporting anonymous

Cryptochecksum:6c41911eabd4b7c54252075bd8434dc4





**Problems;** The most of our issues arose with the configuration of the DNS server because I had configured the DNS server statically to begin with just to have it configured initially but then was able to switch the DNS server over to being dynamically configured by removing the command

DHCP DNS server 4.2.2.2 interface inside

Which statically set the DNS server as 4.2.2.2. In removing that command and clicking box for DNS dynamical box, under the DHCP server tab in configuration on the ASDM.

**Conclusion;** In configuring our firewall for small and medium businesses we have created a perfect configuration for any small business. This will enable proper protection against any threat actors and provide protection for all sensitive information on the network. Through command line commands and utilization of the ASDM GUI it is remarkably simple to protect your small business network.