Configuration of Cisco ASA

and ASDM

# CCNAS Lab 1

Michael Li

10 September 2019

# 

# Purpose

The following lab is purposed as an exercise of setting up physical Cisco ASAs for use in networks with other devices. ASAs are crucial security devices for any network, particularly those that are destined for open access to public networks. This is as ASAs protect the administrator's network from malicious intrusion and attacks originating from the internet. As such this lab is training in the process of installing an ASA in a network, configuring basic commands, and installing its resources through the command line interface (ASDM).

# Background

As mentioned previously, ASAs protect the network from harm and external attacks. However, ASAs do so using firewalls, which when implemented allows for certain users to access the network while uninvited guests from outside the network (without permission) are blocked. It is through this process that an ASA partitions the network into more manageable segments. ASAs also provide antiviral services, which analyzes and eliminates bugs and malware from the network. This prevents said malicious and likely harmful programs from damaging the network. ASAs also provide intrusion prevention, which allows for the network to avoid/mitigate more precise and targeted attacks on the network. Intrusion prevention is inherently proactive. It preemptively identifies potential threats and blocks them before they are immediately dangerous.

Cisco ASAs provide additional Virtual Private Network (VPN) support, which allows for proxying and masking of IP addresses. It does so through tunneling to other domains, and thereby provides security for users in potentially unsafe public/foreign networks by reducing the risk of malicious attacks.

The network is analogous to a prison, or a private mansion estate if we want to go with something more pleasant. The ASA is the security detail. Firewalls are the main gate, or a literal wall (flames for dramatic effect) around the property. The gate only unlocks and swings open for permitted guests, but blocks everyone else. Firewalls, like physical barriers however, can be broken. Antivirus software of the ASA like human guards sweep the estate and detain/neutralize any intruders. Finally, intrusion prevention serves as a detection/radar system. The security guards preemptively scan the areas outside the estate to prevent attacks before they happen.

# Summary

The setup of this lab involved the writing of commands and configurations on text files, after which we would read through, and then paste in the ASA for further testing. The lab used Cisco 5505 ASAs. The network topology was also designed, in which we planned out our IP addressing. This would be used for the configuration of our PC addressing. On the Cisco ASA, an interface was enabled with *https server* functions. A web browser was then used to access the interface’s IP address, where the ASA provided Java and the ASDM resources that would run on it (through a wizard program).

# Commands

**The major commands specific to this lab are as follows:**

**Nameif inside**: ASA refers to the physical interfaces corresponding to virtual interfaces. Configures the interface to face inwards, facing away from the network, when directing traffic.

**Nameif outside**: Configures the interface to face outwards, facing towards the network, when directing traffic.

**username** [username] **privilege** [level] **password** [password]|**secret** [encrypted password]: Configures a login including a static username, a password, and which features it may access based on privilege level.

**Config factor-default**: Restores the factory default configuration.

**Enable password**: Creates password.

# 

# 

# 

# 

# Diagrams

# 

# Configurations

**ciscoasa# show run**

Saved

Serial Number: JMX1142Z1H1

Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz

ASA Version 9.2(4)14

hostname ciscoasa

enable password 8Ry2YjIyt7RRXU24 encrypted

names

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 192.168.1.5-192.168.1.36 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

Cryptochecksum:f043742f4143a7f9c5b7ddea7fd15a87

: end

# 

|  |  |
| --- | --- |
| **Accessing the HTTPS address we configured to the ASA to reach this prompt, where we can then download and install Java and the ASDM, in that order.** |  |
| **Using the ASDM GUI to view all statuses and processes.** |  |

# 

# Problems

This lab despite being completable in one day, was met with issues primarily unrelated to the content itself. Before the initial configuration, the ASAs that were given to us were used from a previous year. This involved ROMMON mode, which required us to break into the ASA and alter user access so that we could gain access. A simple change of the config-register to 0x1 allowed us to solve the problem with a new username and password.

Before we were even able to complete this however, our first ASA did not start up at all. Our main suspicion is that someone else jammed the power plug into the ASA too hard, which led to crippling damage. This led us to switch the ASA out for a different one.

When downloading the ASDM launcher and Java from the https address, we encountered an equipment issue where the WiFi was incredulously slow. After consulting classmates, we found out it was because network activity was cluttering all the bandwidth. The estimated download times were up to 2 hours, and so we had to wait until the internet cleared up a few days later.

# Conclusion

This lab was foundational experience for future work with ASAs. We learned how to set up, wipe, and configure an ASA, despite preconfiguration, hardware, and internet issues. Because networks in the industry vary widely and need to be adaptable at protecting privacy and maintaining security, it is axiomatic that as a class we have acquired an introduction to the ASA.