ASA

Filtering

With FirePOWER

# CCNAS Lab 4

Michael Li

23 January 2020

# Purpose

The following lab is purposed as an exercise of installing FirePOWER on our new ASA 5506 and configuring the software to filter for URLs and malware. This would also involve an effort of finding license-keys and registering software before and after installation. As discussed, ASAs are crucial security devices in networks with access to public networks and provide VPN, firewall, antivirus, and intrusion prevention services that prevent or mitigate malicious attacks. The goal of this lab was to simulate a real environment in which an organization uses the features of an ASA to restrict certain content and software in protection of its interests.

# Background

Cisco’s wide portfolio of products includes ASA FirePOWER Services, which is meant as the “next generation” of firewall technology enclosed within the flagship Cisco ASA. Most notably in our case, is the Cisco 5506. With next generation functions, comes licensing in the ASA-OS and software module like control licenses, protection licenses, advanced malware protection, and URL filtering licenses. The control license allows for user and application control by adding application and user conditions in order to access control rules. Control is dependent on enabling protection. The protection license includes intrusion detection and prevention behavior, as well as file control and security intelligence filtering. AMP Licensing (Advanced Malware Protection) allows for the ASA to perform malware code detections and blocking when code is transmitted over the network. Finally is URL Filtering, which is self-explanatory to the name. It is used in access control rules that can either allow or deny certain traffic from traversing the network based on the URLs/web categories of domains requested by monitored hosts. These categories are labeled by the topics and information contained on said domains, which is provided by Cisco over the cloud in the ASA FirePOWER module. This is essentially an industry-standard feature, where companies and organizations need to filter web traffic to prevent users/hosts to view or interact with potentially harmful or explicit material that will disrupt organizational function, such as video games or pornographic material. Given the nature of the classroom environment, only the former was tested in the lab.

# Summary

For this lab, the default factory settings were first set up on the ASA 5506 via console, after our teacher provided us the device out of the box. We then connected to the ASA over ethernet via ASDM.

We were given four licenses, which were activated through the Configuration > ASA FirePOWER Configuration > Licenses page. The licenses were pasted there in corresponding boxes.

URL filtering was configured through the access control policy via ASDM (under the Configuration > Firewall > Service Policy Rules page). This blocked traffic that fell under the gaming URL category.

The ASA was also configured with a FirePOWER module to analyze all traffic so the URL filtering would actually be applied across all traffic on the network.

The URL filtering was tested by navigating to gaming and non-gaming sites to confirm that the desired sites were blocked.

# Commands

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

**class-map** global-class: Creates a class map along with a corresponding ***match*** *commands, which defines each Layer 3 and Layer 4 traffic class as well as each Layer 7 protocol class. Class maps also allow for the classification of traffic received and transmitted by the ACE. Must contain class map name.*

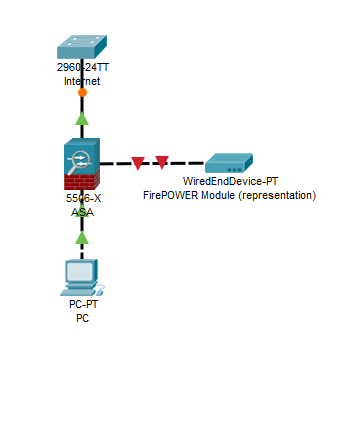
**match** [any|all]: Individual match commands specify the criteria for classifying Layer 3 and layer 4 network traffic as well as the Layer 7 HTTP server load balancing and application protocol-specific fields. The ACE evaluates the packets for certain criteria of a class and forwards the packet according to traffic policy. Packets failing to meet matching criteria are classified as members of the default traffic class.

**policy-map** global-policy: Creates a policy map which refers to the class maps and identifies a series of actions to perform based on the traffic match criteria. This creates the traffic policy which implements specific ACE functions associated with a traffic class.

**class** global-class: Specifies a Layer 3 and Layer 4 traffic class created with the **class-map** to associate network traffic with the traffic policy. Done in policy map configuration mode.

**Sfr** fail-open: Sends traffic to the ASA FirePOWER module where “fail-open” sets the ASA to allow all traffic through, uninspected if the module is unavailable.

# Diagrams



|  |  |  |
| --- | --- | --- |
| **Device** | **Interface** | **IP Address** |
| PC | NIC | DHCP |
| ASA | Internal/External | Internal:192.168.1.1  External: DHCP |
| FirePOWER | Management Port | 192.168.1.3 |

|  |  |
| --- | --- |
|  | Cisco ASA 5506 device information displayed on the home page of ASDM |
|  | The corresponding box for the insertion of license keys. License keys are downloaded and accessed as files provided by the instructor. |
|  | A display of all ASA5506 licenses installed on our device. |
|  | Configuring service policy rules to direct traffic through the FirePOWER module. Note that this option should be set to permit traffic so that traffic flows through the FirePOWER module properly by default (see problems section for our experience with this) |
|  | Example of editing a policy rule. This page allows us to configure a rule to block URLs based on category filters. |
|  | Displays all configured rules for filtering. |
|  | Displays all server policy rules configured on the Firewall. Note this is where our glocal-class policy rule is displayed (configured via the CLI as explained elsewhere in this report). |
|  | This is a setup of our URL filtering settings. It reports filtering updates and allows us to toggle/enable URL filtering. It also allows us to query for unknown URLs as well as to setup automatic updates so new updated information on domains can be provided to our policy rule categories. |
|  | A close-up view of our access control policy. All details were configured as explained/displayed. |
|  | Successful denial of battle.net, a popular gaming-related site. |

# Configurations

**ASA# show run**

: Serial Number: JAD232301UT

: Hardware: ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)

:

ASA Version 9.8(2)

hostname ciscoasa

enable password $sha512$5000$00UqFXI0OBoW35gONKgdIg==$QIhzIvikVlOBUtw81+Apfw== pbkdf2

names

interface GigabitEthernet1/1

nameif outside

security-level 0

ip address dhcp setroute

interface GigabitEthernet1/2

bridge-group 1

nameif inside\_1

security-level 100

interface GigabitEthernet1/3

bridge-group 1

nameif inside\_2

security-level 100

interface GigabitEthernet1/4

bridge-group 1

nameif inside\_3

security-level 100

interface GigabitEthernet1/5

bridge-group 1

nameif inside\_4

security-level 100

interface GigabitEthernet1/6

bridge-group 1

nameif inside\_5

security-level 100

interface GigabitEthernet1/7

bridge-group 1

nameif inside\_6

security-level 100

interface GigabitEthernet1/8

bridge-group 1

nameif inside\_7

security-level 100

interface Management1/1

management-only

no nameif

no security-level

no ip address

interface BVI1

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0

ftp mode passive

same-security-traffic permit inter-interface

object network obj\_any1

subnet 0.0.0.0 0.0.0.0

object network obj\_any2

subnet 0.0.0.0 0.0.0.0

object network obj\_any3

subnet 0.0.0.0 0.0.0.0

object network obj\_any4

subnet 0.0.0.0 0.0.0.0

object network obj\_any5

subnet 0.0.0.0 0.0.0.0

object network obj\_any6

subnet 0.0.0.0 0.0.0.0

object network obj\_any7

subnet 0.0.0.0 0.0.0.0

pager lines 24

logging asdm informational

mtu outside 1500

mtu inside\_1 1500

mtu inside\_2 1500

mtu inside\_3 1500

mtu inside\_4 1500

mtu inside\_5 1500

mtu inside\_6 1500

mtu inside\_7 1500

icmp unreachable rate-limit 1 burst-size 1

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

arp rate-limit 16384

object network obj\_any1

nat (inside\_1,outside) dynamic interface

object network obj\_any2

nat (inside\_2,outside) dynamic interface

object network obj\_any3

nat (inside\_3,outside) dynamic interface

object network obj\_any4

nat (inside\_4,outside) dynamic interface

object network obj\_any5

nat (inside\_5,outside) dynamic interface

object network obj\_any6

nat (inside\_6,outside) dynamic interface

object network obj\_any7

nat (inside\_7,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 sctp 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

timeout conn-holddown 0:00:15

timeout igp stale-route 0:01:10

user-identity default-domain LOCAL

aaa authentication login-history

http server enable

http 192.168.1.0 255.255.255.0 inside\_1

http 192.168.1.0 255.255.255.0 inside\_2

http 192.168.1.0 255.255.255.0 inside\_3

http 192.168.1.0 255.255.255.0 inside\_4

http 192.168.1.0 255.255.255.0 inside\_5

http 192.168.1.0 255.255.255.0 inside\_6

http 192.168.1.0 255.255.255.0 inside\_7

no snmp-server location

no snmp-server contact

service sw-reset-button

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpool policy

telnet timeout 5

ssh stricthostkeycheck

ssh timeout 5

ssh key-exchange group dh-group1-sha1

console timeout 0

dhcpd auto\_config outside

dhcpd address 192.168.1.5-192.168.1.254 inside

dhcpd enable inside

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

dynamic-access-policy-record DfltAccessPolicy

class-map global-class

match any

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

no tcp-inspection

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

class global-class

sfr fail-open

service-policy global\_policy global

prompt hostname context

no call-home reporting anonymous

Cryptochecksum:f37f4b5a923e55dd83dfce49cbee4618

# Problems

While the lab was intuitive and straightforward, it wasn’t without its issues. Strangely by Cisco’s design, the FirePOWER module is physically separate from the ASA itself. This was a fact that we were initially unaware of, which required us to use a physical cable from an ASA port to the FirePOWER management port. This did cause quite a bit of difficulty.

We also struggled with licensing. Our instructor accidentally provided one license with 28 years of time before expiration, instead of providing 28 licenses each with one year of elapsed time before expiration. This led to licenses not registering on our ASAs.

There was also a struggle involving the URL filtering. We were under the assumption that the ASA FirePOWER module process traffic automatically through the network, but it was later found that traffic needed to be forwarded from the ASA 5506 for analysis. When we realized this and attempted to configure this via ASDM under the Configuration > Firewall > Service Policy Rules page, we also encountered an unusual problem: a dialogue box would constantly pop up, preventing us from making and saving the changes. This forced us to diverge from ASDM and onto the command line interface for the duration of this part of the lab. It arguably would’ve been more convenient to have stayed on ASDM.

What was notable however is that the dialogue box would still pop up on the Service Policy rules when we tried to edit the rule, even after we configured everything.

# Conclusion

This lab served as a solid introduction into the implementation of the FirePOWER module on a new Cisco 5506. Although most of the lab was straightforward, its complications provided a good demonstration of the available features of FirePOWER as well as how to utilize them.