Upgrading Cisco ASA

and ASDM

# CCNAS Lab 2

Michael Li

10 September 2019

# 

# Purpose

The following lab is purposed as an exercise of updating the software of a Cisco 5505 ASA, including ASDM. 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 for updating an ASA and ensuring that it has all the latest features necessary for ensuring the security of a network.

# 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.

ASAs run on ASA software and use ASDM for various purposes. With both residing on flash memory, this lab uses tftp to upload software images through the CLI and/or through ASDM to update older software images.

# Summary

The setup of this lab required us to obtain software images on our computers, with which we would then upload into the Cisco ASA with TFTP/ASDM. This process self-evidently required us to configure a TFTP server through which the upgrading process would be conducted. Software images were verified with show image commands. The lab used Cisco 5505 ASAs.

Once a new image is on the ASA, ASDM detects a version difference and prompts the user to close ASDM and redownload the newer version (through a web browser on the corresponding IP address like in the previous lab.

This lab being an image upgrade process was unlike the usual lab. Whereas a typical lab would involve the creation of a configuration on a text file for a later duplication into the necessary devices, this update was more of a slow manual process rather than programming. Hence, there are no succinct configurations, but rather a configuration process.

# Commands

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

**copy tftp**[:[[//location] [/tftp\_pathname]]] [[flash/disk0][:[image | asdm]]]: Downloads software image into the Flash memory of the Cisco ASA through TFTP

**boot system** [flash:/disk0:]/[software image name]: Sets an image as the bootup image and specifies a ASDM image file.

**write memory**: Saves active configuration to Flash memory

**asdm image** [[flash/disk0][:[image | asdm]]]**:**Sets an ASDM image as the operating ASDM image.

**No asdm image** [[flash/disk0][:[image | asdm]]]**:**Removes an ASDM image from usage.

**Show version:**Displays current image with which the ASA is booted

**Show asdm image:**Displays the current ASDM image on the Cisco ASA

.

# 

# 

# 

# Diagrams

# 

# Configuration Process

**\*Note that rather than having defined programming, the ASA was simply configured through the commands in the “Commands” section**

disk0:/asdm-762.bin

disk0:/asa924-14-k8.bin

disk0:/asa924-33-k8.bin

disk0:/asdm-7101.bin

**ciscoasa#** show version | include image

System image file is "disk0:/asa924-14-k8.bin"

**ciscoasa#** show asdm image

Device Manager image file, disk0:/asdm-7101.bin

# 

|  |  |
| --- | --- |
| **Using ASDM to transfer files (ASA and ASDM images) from PC storage to ASA Flash memory.**  **(Note this process was ultimately unsuccessful, which led us to use the CLI instead)** |  |
| **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.**  **(Note the screenshots represent a previous version of ASDM)** |  |

# 

# Problems

This lab despite being completable in an hour, did face a couple issues that delayed instructor approval. One thing being ASDM not successfully uploading the ASA and ASDM images. What we came to learn was that simply running a transfer and deleting previous images does not upgrade the software on the device, rather, far from it. Although we eventually reached the goal of this lab, we did not do so through the ASDM GUI, but through a more traditional CLI approach.

We managed to upload everything via the *copy tftp* command, however, whenever we reloaded the ASA and downloaded a new copy of ASDm from the web browser, we were unable to see the new software images indicated in the ASDM. In various cases, the *show version* and *show image* commands would indicate the correct results, but the ASDM would not. Other times the opposite was true, ASDM would show the correct software images but CLI commands would not yield the same result.

After using the *no asdm image* command to remove and replace software images repeatedly in frustration, we resolved the problem by using the *copy run start* command as well as the *write memory* command.

# Conclusion

This lab was foundational experience for future work with ASAs. We learned how to use TFTP in the CLI to upgrade the software images of an ASA. 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 a skill necessary for the maintenance of an ASA.