ASA Firewall Configuration Lab Report

IR.2406 – Network Security

Ilias Bezzaz, Selim Ahmine, Elias Ait Khelifa
ISEP

Introduction

This document summarizes the results and analysis of our practical lab session dedicated to the configuration of the Cisco ASA 5505 firewall using CLI. This hands-on exercise is part of the IR.2406 – Network Security course. Our goal was to understand and apply core security configurations such as routing, NAT, DHCP, VLAN segmentation, access control lists, and remote management over SSH.

The work was conducted by a group of three cybersecurity engineering students: Ilias Bezzaz, Selim Ahmine, and Elias Ait Khelifa.

PART 2

What software version is this ASA running?

The ASA is running **Cisco Adaptive Security Appliance Software Version 8.4(2)**. This version supports modern security features such as object-based NAT, modular policy framework, and enhanced CLI syntax.

What is the name of the system image file and from where was it loaded?

- **System image:** `asa842-k8.bin`
- **Loaded from:** `disk0:/`

What version of ASDM is this ASA running?

The ASA runs **ASDM Version 6.4(5)**, providing a GUI alternative to CLI for ASA configuration and monitoring.

How much RAM does this ASA have?

The ASA 5505 is equipped with **512 MB** of RAM, which allows it to handle stateful inspection, ASDM services, and NAT translations efficiently for a small network environment.

How much flash memory does this ASA have?

The ASA has **128 MB** of internal ATA Compact Flash memory (`128573440 bytes`), used for storing system images, ASDM, and configuration files.

How many Ethernet ports does this ASA have?

There are **8 Ethernet ports**, labeled from `Ethernet0/0` to `Ethernet0/7`. Ports E0/6 and E0/7 support Power over Ethernet (PoE).

What type of license does this ASA have?

The device is running a **Base License**, which restricts some advanced features (such as high availability or multiple context mode).

How many VLANs can be created with this license?

Up to **3 VLANs** can be configured simultaneously. This includes the inside, outside, and one optional DMZ interface. The third VLAN (DMZ) requires a `no forward` command to isolate it from one of the others.

What is another name for `flash:`?

The alias `disk0:` is an alternative name for `flash:`.

PART 4

STEP 1

a. Was the ping from ASA to R1 G0/0 successful? No. The ASA had not yet been configured with a default route, so it had no knowledge of networks beyond its directly connected interfaces.

b. Was the ping from ASA to R1 S0/0/0 successful? No. As with the previous case, the ASA did not have a route to the 10.1.1.0/30 network. Without a proper routing table, the packet was dropped.

e. Was the ping from ASA to R1 S0/0/0 successful after adding a default route? Yes. Once the default route was added, the ASA was able to forward the packet to R1, which routed it towards its serial interface.

STEP 2

f. Were pings from PC-B to R1 G0/0 successful? No. At this point, NAT (specifically PAT) had not been configured yet. The ASA forwarded packets with unroutable private IP addresses (192.168.1.X), which were rejected by R1.

PART 5

Were you able to configure the full DHCP pool from 192.168.1.5 to 192.168.1.100? No. Due to Base License restrictions, the ASA only allows a DHCP pool of 32 addresses. We therefore reduced the range to `192.168.1.5 { 192.168.1.36`, which respects this limitation while allowing dynamic IP assignment to internal hosts.

PART 6 - Reflection

1. How does the configuration of the ASA firewall differ from that of an ISR?

The ASA employs a security-centric architecture:

- **Zone logic:** Interfaces are assigned *security levels* (0–100) rather than belonging to IOS-style zones.

- **Stateful inspection:** ASA implements MPF (Modular Policy Framework) to inspect traffic by protocol.
- **NAT by objects:** The NAT configuration relies on logical network objects for clarity and scalability.
- **Command set:** Although similar to IOS, ASA commands differ slightly and focus more on filtering and inspection than routing.

In contrast, an ISR uses traditional IOS commands, class-based QoS, and often integrates firewall rules via Zone-Based Firewall (ZBF).

2. What does the ASA use to define address translation and what is the benefit?

ASA uses **network objects** and **object groups** to define NAT rules. This allows:

- Centralized configuration of both the network and its translation rule.
- Better readability and scalability of the NAT configuration.
- Easier adaptation for static, dynamic, identity or twice NAT.

3. How does the ASA 5505 use logical and physical interfaces to manage security and how does this differ from other ASA models?

The ASA 5505 uses **VLAN interfaces** (Layer 3 logical) mapped to **Layer 2 physical ports**. Security policies, IP addressing, and NAT apply to VLANs, not to physical interfaces. In contrast, larger ASA models (e.g., 5510+) have routed physical interfaces, allowing direct IP assignment and zoning without VLAN abstraction. The ASA 5505 behaves more like a managed switch with firewall capabilities.