Lesson Proper for Week 17

CISCO ASA PORTFOLIO

The purpose of a firewall is to filter incoming and outgoing traffic between networks. The ASA is a family of next-generation firewalls from Cisco systems. The ASA is a standalone appliance that provides stateful and packet filtering, **Network Address Translation (NAT)**, routing, **Dynamic Host Configuration Protocol (DHCP)**, **Virtual Private Network (VPN)** capabilities, botnet filtering, **Advanced Malware Protection (AMP)**, and deep packet inspection. Those are only a few of the features and services it offers. In the next section, we will dive a bit deeper into discussing the features of the ASA and its abilities to prevent threats from entering a network/organization.

The following is a picture of Cisco ASA 5505:

The ASA comes in many different shapes and sizes to fit business needs. Some models include: 5505, 5510, 5520, 5540, 5550, 5506-X, 5506W-H, 5506H-X, 5508-X, 5516-X, 5525-X, 5545-X, and 5555-X. You may ask yourself, what's the main difference between the Cisco ASA 5500 series appliance and the newer Cisco ASA 5500-X series? To answer that question, Cisco has developed a new technology called **FirePOWER**, which is supported on the 5500-X appliances.

You may have noticed each ASA has a different model number. The model number defines the capacity for the number of nodes and bandwidth it can support in an organization/network. Therefore, each ASA is designed for a particular network size, ranging from small office, branch office, medium-tolarge networks, to internet edge and datacenter networks.

ASA FEATURES

In the previous section, we mentioned some of the features and services of the ASA. Here, we are going to discuss the key features and services in the ASA and how they can assist your organization and fit business needs. Whether you are a student, a network security engineer, a cyber security professional, or simply an enthusiast, understanding the functionality of the ASA will be helpful in the journey ahead.

Let's begin!

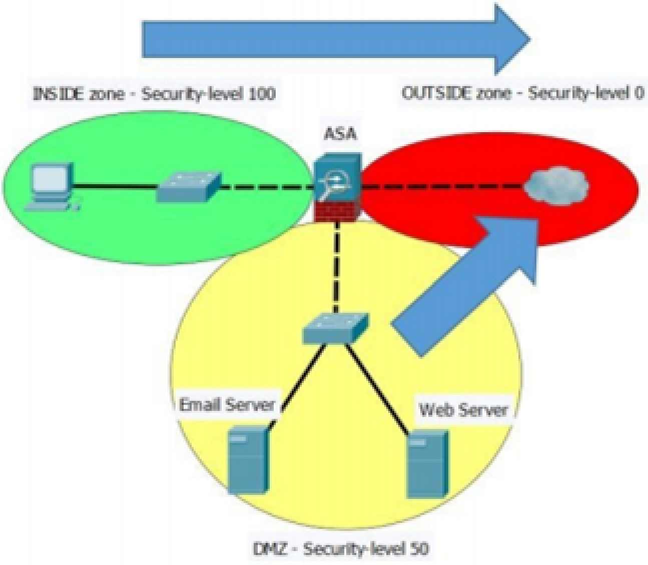
First, let's discuss a few things about the ASA and how it determines (by default) whether traffic is allowed to flow from one interface to another. Each interface on the ASA is assigned to a network ,or what is better known as a zone. A zone is simply an area on the network. There are typically three **zones**: the **INSIDE** zone, the **OUTSIDE** zone, and the Demilitarized zone. Each zone has a security level defined by a number ranging from 0 to 100. The number determines the trust level of a zone and if traffic is allowed to flow between zones, whether unidirectional or bidirectional.

How exactly does the security level play a role in each zone? Let's break this down a bit further: a zone with a 100 security level is a fully trusted zone, such as your private **Local Area Network (LAN).** An untrusted zone, such as the internet, typically has a security level of 0. The DMZ is the semi-trusted area in your network. Within the DMZ, you'll find your public servers. In a typical DMZ, your organization may have several servers that require a direct internet connection, in other words, they are public-facing. The purpose of the DMZ is to allow partial access from the internet to the DMZ only, and not access from the internet to the private LAN. The DMZ usually has a security level ranging from 1 to 99.

Stateful filtering

Stateful filtering is a feature that monitors traffic originating from one zone and moving to another. It keeps track of this information and would allow only the returning traffic through the ASA.

Traffic originating from a zone with a higher security level, such as the **INSIDE zone (100),** is allowed to go to a zone with a lower security level, such as the OUTSIDE (0) and DMZ (50), and the return traffic is allowed because the ASA keeps track of the flows of traffic in a state table (stateful filtering):


INSIDE zone - Security-level 100
OUTSIDE zone - Security-level 0
ASA
Email Server
Web Server
DMZ - Security-level 50

However, traffic originating from the **OUTSIDE (0)** zone is not allowed to reach the **INSIDE (100)** zone or the **DMZ (50)** by default, nor is traffic originating from the DMZ (50) allowed to access the **INSIDE (100)** zone.

Packet Filtering

Packet filtering enables an ASA to either permit or deny traffic based on a packet's source, and/or destination IP address, and/or source, and destination Port number. The ASA can achieve this by using an **Access Control List (ACL).**

For example, let say you want to restrict users from the 192.168.1.0/24 network from visiting the Cisco website. We know a web server typically uses port 80 (this would be our destination port) and the IP address for https://www.cisco.com/ is 23.37.75.188 (our destination IP address). Therefore, we would create an ACL to achieve this function on the ASA. Assuming our internal network is 192.168.1.0/24, our ACL would typically be access-list 100 deny tcp 192.168.1.0 0.0.0.255 23.37.75.188 255.255.255.255 eq 80. Don't worry, we'll discuss ACLs in the later chapters.

Network Address Translation

Network Address Translation (NAT) allows private IP addresses (RFC 1918) to be translated into another IP address. An example would be devices, such as computers, that are sitting on the private LAN trying to access https://www.cisco.co m/ on the internet. Because their private IP addresses are non-routable on the internet, each device would require a public IP address. Using NAT on the Cisco router or ASA, the appliance allows devices with private IP addresses to be translated to the public IP address (which is on the internet-facing port). NAT allows a network to be hidden behind a single IP address for security purposes. It is also used to conserve the public IPv4 address space.

Routing

The ASA has routing capabilities like a router. It has the ability to exchange routing information for **Routing Information Protocol (RIP)**, **Enhanced Interior Gateway Routing Protocol (EIGRP),** and **Open Shortest Path First (OSPF)**. The ASA supports static routing.

Dynamic Host Configuration Protocol

The ASA can function as both a **Dynamic Host Configuration Protocol (DHCP)** server and a DHCP client for receiving an IP address on its interface(s). The DHCP server enables the ASA to automatically assign dynamic IP addresses, subnet mask, default-gateway, DNS server, and so on to clients or any device that is requesting an IP address on the network. The DHCP server can be useful for small companies and branch offices.

Virtual Private Network

A Virtual Private Network (VPN) allows a secure connection between two devices/networks over an untrusted network. The ASA can support both an **IPSec** (short for, **Internet Protocol Security**) and **SSL** (short for**, Secure Sockets Layer**). It has the ability to establish site-to-site and remote access VPNs.

Botnet filtering

A bot (robot) is a small piece of malicious code that infects a device, making it a zombie machine. The bot listens for instruction from a **Command and Control (CnC)** server. A group of zombies makes up a botnet (bot network) and they can all be controlled from a single CnC server to perform malicious activities.

The botnet filtering on the ASA is a license-based service from Cisco that allows the firewall to monitor, detect, and prevent such threats.

Advanced Malware Protection

With the evolution of **Advanced Persistent Threats (APTs)**, the Cisco **Advanced Malware Protection (AMP)** provides malware protection before, during, and after an attack. AMO is a feature that provides next-generation abilities in the ASAs (5500-X models).

Authentication, authorization, and accounting

The Cisco ASA support **authentication, authorization,** and **accounting (AAA).** This feature allows the ASA to act as a local AAA server or can query a remote AAA appliance, such as a **Remote Authentication Dial-In User Service (RADIUS)** or a **Terminal Access Controller Access-Control System Plus (TACACS+)** server.

Class map and policy map

The ASA uses class map to identify traffic, IP addresses, Layer 4 protocols, or application protocols. A policy map is used to perform an action (permit, deny, and so on). A service policy is a used to apply a policy on either all interfaces or a single interface on the ASA. To give an example, let's say we want to block all outgoing HTTP tr first we would create a class map to identify the HTTP traffic, then a policy map to deny/drop the outgoing tra and finally use a service policy to apply the policy on the interface of our choosing.

◀ Preliminary Activity for Week 17

Jump to...

Analysis, Application, and Exploration for Week 17 ▶

Navigation

- Home
- Dashboard
  - Site pages
  - My courses
    - 121 - CC106
    - 121 - BPM101 / DM103
    - 121 - OAELEC2
    - 121 - ITE3
    - 121 - MUL101
    - 121 - ITSP2B
      - Participants
      - Grades
      - General
      - 01 Exploring Security Threats
      - 02 Delving into Security Toolkits
      - 03 Intrusion Prevention System
      - 04 Understanding Security Policies I
      - 05 Understanding Security Policies II
      - 06 - Preliminary Examination
      - 07 Deep Diving into Cryptography
      - 08 Deep Diving into Cryptography: Types of Cipher
      - 09 Implementing the AAA Framework
      - 10 Implementing the AAA Framework: Implementing A...
      - 11 Securing the Control and Management Planes
      - 12 - Midterm Examination
      - 13 Protecting Layer 2 Protocols
      - 14 Protecting the Switch Infrastructure
      - 15 Exploring Firewall Technologies I
      - 16 Exploring Firewall Technologies II
      - 17 Cisco ASA
        - Preliminary Activity for Week 17
        - **Lesson Proper for Week 17**
        - Analysis, Application, and Exploration for Week 17
        - Generalization for Week 17

- Evaluation for Week 17
- Assignment for Week 17

121 - WEB101 / CCS3218

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission***.

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

2nd Semester Enrollment

visit www.bcp.edu.ph
Enrollment registration is now Ongoing
For 2nd Semester SY 2021 - 2022
We are accepting new students, returnees and transferees.
"Be trained to be the best,
Be linked to success"
bcp-inquire@bcp.edu.ph
(8)442-8601 | (8)518-8050

Activities

- Assignments
- Forums
- Quizzes
- Resources

Bestlink College of the Philippines
College Department

Powered byeLearning Commons