Packet Tracer Basic ASA lab

The purpose of this lab is to provide a better understanding of Cisco’s ASA 5505 Adaptive Security Appliance; The Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. In this lab we will Packet Tracer 6.1. to learn how to configure the ASA as a basic Firewall. This knowledge is essential to passing the CCNA Security exam and will be used in daily in your position as a Cisco network engineer.

The Cisco ASA 5505 is a next-generation, full-featured security appliance for small business, branch office, and enterprise teleworker environments. The Cisco ASA 5505 delivers high-performance firewall, SSL and IPsec VPN, and rich networking services in a modular, "plug-and-play" appliance. Using the integrated Cisco ASDM, the Cisco ASA 5505 can be rapidly deployed and easily managed, enabling businesses to minimize operations costs. The Cisco ASA 5505 features a flexible 8-port 10/100 Fast Ethernet switch, whose ports can be dynamically grouped to create up to three separate VLANs for home, business, and Internet traffic for improved network segmentation and security. The Cisco ASA 5505 provides two Power over Ethernet (PoE) ports, simplifying the deployment of Cisco IP phones with zero-touch secure voice over IP (VoIP) capabilities, as well as the deployment of external wireless access points for extended network mobility. A high-performance intrusion prevention and worm mitigation service is available with the addition of the AIP SSC. Multiple USB ports can be used to enable additional services and capabilities as they are needed.

# Learning Objectives:

* Configure interfaces and vlans.
* Configure dhcp.
* Configure Objects and object-groups.
* Configure NAT rules.
* Configure class-map.
* Configure policy-map.
* Configure service-policy.

# Lab Task:

The internet is preconfigured in this lab and will require no additional configuration.

* DNS Server 209.165.200.10/48.
* WEB server 209.165.200.11. (freecnalab.com).

## R1:

1. Configure the interfaces on R1 as shown in the network diagram.
2. Configure a default route on R1.

## R2:

1. Configure the interfaces on R2 as shown in the network diagram.
2. Configure a default route on R2.

## ASA:

1. Assign the interface to vlans.
2. Configure the VLAN interfaces with IP address, interface name and security level.
3. Configure a default route to allow the inside devices to access the internet.
4. Configure an object for all inside subnets.
5. Configure a NAT rule to translate inside addresses to an outside address.
6. Create a global policy named global-policy, to inspect traffic and filter the traffic to include the following.
7. DNS
8. FTP
9. H323
10. HTTP
11. ICMO
12. TFTP
13. Apply the global policy as a service-policy.

## Verify configuration:

1. From the Local PC-1 ping 209.165.200.11. (this may require doing it twice)
2. From the Local PC-1 ping 172.16.3.3. (this may require doing it twice)
3. From the Remote PC ping 209.165.200.11. (this may require doing it twice)
4. From the Remote PC ping 192.168.1.100.
5. From the Local PC-1 open the desktop and browse to freeccnalab.com.
6. From the Remote PC open the desktop and browse to freeccnalab.com.
7. From the Remote PC open the desktop and browse to 192.168.1.100.