Packet Tracer DMZ ASA Lab

The purpose of this lab is to provide a more advanced 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 with the addition of a third zone referred to as a DMZ. This knowledge is essential to passing the CCNA Security exam and will be used in daily in your position as a Cisco network engineer.

# DMZ:

In computer security, a DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical sub network that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network.

The ASA 5505 implemented in Cisco’s Packet Tracer is the smallest model in the newest 5500 series of Cisco firewalls. It is a great product for small businesses (5-10 employees) or even for home network use. However, if you need to create a DMZ zone (in addition to your Inside and Outside zones) in order to install a publicly accessible server (e.g. WEB server, MAIL server etc.), then the default basic license provided by Packet Tracer 6.1 won’t work for you. The basic license does not allow more than 2 security zones. You will need to upgrade to “Security Plus” license which also enhances some other firewall parameters (more firewall connections, more remote access VPN sessions, and trunking with 20 VLANs).

Due to the above limitations in our lab we will use Packet Tracer to configure a small security network with the following requirements:

* Computers on the inside interface will be allowed to access the web server freeccnalab.com in the internet.
* Computers on the inside will also have access to the SarePoint server in the dmz.
* Remote computers will also be allowed to access the internet but will not be allowed to access computers on the inside or the SarePoint server on the dmz interface.
* The dmz will also act as a guest hotspot allowing guest computers to connect to the internet and the SharePoint server via a wireless interface.
* Guest computers will not have access to computers or servers on the inside interface.

# 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 and ISP router 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 Inside and Outside 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. ICMP
12. TFTP
13. Apply the global policy as a service-policy.

## DMZ:

1. Assign the DMZ interface to vlans.
2. Configure the VLAN interfaces with IP address, interface name and security level.
3. Configure an object for all DMZ subnets.
4. Configure a NAT rule to translate DMZ addresses to an outside address.

## Wireless:

1. Configure the wireless AP with SSID Public-Hotspot and set the WPA2-PSK password to CCNALabs.
2. Configure the Laptop computers to connect to the wireless network.

## Verify configuration:

Using the following test insure the lab meets the above requirements.

### Inside:

1. From the Local PC-1 ping 209.165.200.11. (this may require doing it twice)
2. From the Local PC-1 ping 192.168.1.200. (this may require doing it twice)
3. From the Local PC-1 open the desktop and browse to freeccnalab.com
4. From the Local PC-1 open the desktop and browse to SharePoint.

### DMZ:

1. From the Local LT-1 ping 192.168.2.200. (this may require doing it twice)
2. From the Local LT-1 ping 209.165.200.11. (this may require doing it twice)
3. From the Local PC-1 open the desktop and browse to freeccnalab.com.
4. From the Local PC-1 open the desktop and browse to Local.

### Remote:

1. From the Remote PC ping 209.165.200.11. (this may require doing it twice)
2. From the Remote PC ping 192.168.1.200.
3. From the Remote PC ping 192.168.2.200.
4. From the Remote PC open the desktop and browse to freeccnalab.com.
5. From the Remote PC open the desktop and browse to SharePoint.
6. From the Remote PC open the desktop and browse to Local.