ASA

Home Router

# CCNAS Lab 3

Michael Li

16 October 2019

# 

# Purpose

The following lab is purposed as an exercise of setting up physical Cisco ASAs for use in home networks, potentially as superior albeit expensive replacements for home routers. As discussed, ASAs are crucial security devices in networks with access to public networks and provide VPN, firewall, antivirus, and intrusion prevention services that prevent or mitigate malicious attacks. The goal of this lab was to simulate a real environment in which a Cisco ASA implements DHCP and DNS to provide a PC access to the internet given the proper wired connections.

# Background

As mentioned previously, ASAs (in our case, the Cisco 5505 ASA) 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. 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.

Specific to this lab however, are DHCP and DNS. DHCP (Dynamic Host Configuration Protocol) is a network management protocol that dynamically manages and automatically assigns IP addresses from a pool of addresses to necessary devices (usually by request). DNS operates similar to a phone book/language compiler whose main focus is to convert domain hostnames like “.com” sites to IP addresses that network devices can forward packets towards.

This lab is previously explored territory, however, the contents are now mixed together with the management of ASAs.

# Summary

As this lab is chiefly focused on DHCP and DNS, DHCP was used as an emulation of an ISP on a private network, whereas the ASA would serve a smaller group while a larger DHCP pool would serve a larger population of clients. DHCP was used on the ASA to automatically assign static addresses do devices in our network (the PC).

The setup of this lab involved the writing of commands and configurations on text files, after which we would read through, and then paste in the ASA for further testing. The lab used Cisco 5505 ASAs. The network topology was also designed, in which we planned out our IP addressing. This would be used for the configuration of our PC addressing. On the Cisco ASA, an interface was enabled with DHCP functions. A web browser on a PC addressed using DHCP was then used to access the internet through the ASA.

# Commands

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

**object network** *obj\_name*: Specifies mapped addresses that the administrator wishes to translate to, and configures network object *obj\_name.*

**object-group network** *group\_name*: Specifies mapped addresses that the administrator wishes to translate to, and configures network object group *group\_name.*

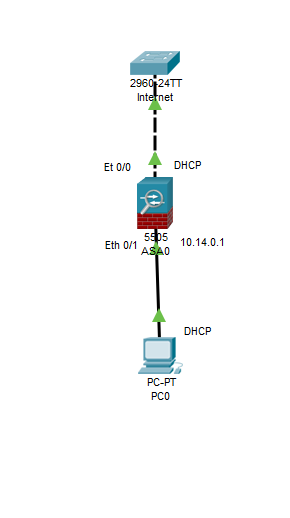
**nat** [(*real\_ifc*,*mapped\_ifc*)] **dynamic** *mapped\_obj* [interface] [dns]: Configures dynamic NAT for object IP addresses (component of command configuring DNS is necessary here)

**ip address dhcp**: Configures an interface with a DHCP-assigned IP address

**ip address dhcp setroute**: Configures a next hop for the default gateway to reach the gateway address provided through DHCP.

# 

# Diagrams



|  |  |  |
| --- | --- | --- |
| **Device** | **Interface** | **IP Address** |
| PC - 0 | NIC | DHCP |
| ASA 0 | Eth 0/1 | 10.14.0/1 |
| ASA 0 | Eth 0/0 | DHCP |

# Configurations

**ASA# show run**

ASA Version 8.4(4)1

hostname ASA

names

ddns update method ddns-2

ddns both

interface Ethernet0/0

switchport access vlan 2

interface Vlan1

nameif inside

security-level 100

ip address 10.14.0.1 255.255.255.0

ASA Home Router Michael Li 5

interface Vlan2

nameif outside

security-level 0

ip address dhcp setroute

ftp mode passive

dns domain-lookup inside

object network obj\_any

subnet 0.0.0.0 0.0.0.0

object network INSIDE\_SUBNET

subnet 10.14.0.0 255.255.255.0

object-group icmp-type ALLOW-ICMP

icmp-object echo-reply

icmp-object time-exceeded

icmp-object unreachable

icmp-object traceroute

access-list INBOUND extended permit icmp any any object-group ALLOW-

ICMP

pager lines 24

logging asdm informational

mtu inside 1500

mtu outside 1500

icmp unreachable rate-limit 1 burst-size 1

no asdm history enable

arp timeout 14400

nat (inside,outside) source dynamic any interface dns

object network obj\_any

nat (inside,outside) dynamic interface

object network INSIDE\_SUBNET

nat (inside,outside) dynamic interface

access-group INBOUND in interface outside

user-identity default-domain LOCAL

http server enable

http 10.14.0.0 255.255.255.0 inside

no snmp-server location

no snmp-server contact

telnet timeout 5

ssh timeout 5

ssh key-exchange group dh-group1-sha1

console timeout 0

dhcpd auto\_config outside

dhcpd address 10.14.0.2-10.14.0.33 inside

dhcpd enable inside

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

webvpn

username Cisco password .n4XRQ0R0.jqeGHq encrypted

class-map inspection\_default

match default-inspection-traffic

policy-map type inspect dns preset\_dns\_map

parameters

message-length maximum client auto

ASA Home Router Michael Li 6

message-length maximum 512

policy-map global\_policy

class inspection\_default

inspect dns preset\_dns\_map

inspect ftp

inspect h323 h225

inspect h323 ras

inspect rsh

inspect rtsp

inspect esmtp

inspect sqlnet

inspect skinny

inspect sunrpc

inspect xdmcp

inspect sip

inspect netbios

inspect tftp

inspect ip-options

service-policy global\_policy global

prompt hostname context

# Problems

This lab was mainly plagued with command use errors. The content of this lab, namely DHCP, was relatively old content and the commands necessary for how to configure them properly were unclear/foggy in memory, and so basic research had to be done. This also applied to usage of DNS, particularly with the NAT command.

A number of our labmates attempted to implement dynamic DNS, which allows for a temporary IP address to be assigned to a server by an ISP every time a new connection to the internet is established. Static DNS on the other hand keeps everything fixed for a particular domain. The issue was for this lab was that we did not want the features of dynamic DNS, as a home router would only need to conserve private IPs for one publicly used one.

While this issue with dynamic DNS did very much confuse us in this process, we did manage to avoid the same trap.

# Conclusion

This lab was an interesting emulation of a daily necessity, and we gained insight into how home routers serve their function. We learned how to set up and configure an ASA with DHCP and DNS to run as a home router and provide devices on a private network with an internet connection. Though DHCP commands and dynamic DNS acted as minor obstacles, we learned a foundational skill for providing an internet connection to a network along with the security features of an ASA (firewall, antivirus, etc.).