|  |  |
| --- | --- |
| Set up ASA 5505 for Internet Connection |  |
|  |  |
|  | |  | | --- | | 10/07/2021CISCO Cybersecurity­ | | Guanzhen Qian | |
|  |  |
|  |  |

**Purpose**

In this lab, we will configure the Cisco Adaptive Security Appliance (ASA) firewall to internet with console connection and ASDM access. The ASDM will work as a default gateway for the PC to connect to the ISP. The purpose of this lab is to understand how to set up an ASA firewall in a SOHO networking environment. This is lab shows how a SOHO owner may set up a physical firewall to protect the networking appliances from unwanted accesses and viruses.

**Background**

Cisco Adaptive Security Appliance (ASA) firewall protects corporate networks and data centers of all sizes. A firewall is a security system designed to block unauthorized access to a network and malicious software. Firewalls analyze network traffics, and it is configured to only accept authorized traffic. Firewalls can be software or hardware. A software firewall is a program on a device that works through ports and applications. A hardware firewall is a physical device placed between network and gateway or network and end devices. Without a firewall, end devices accept every connection into networks.

Cisco Adaptive Security Device Manager (ASDM) graphic user interface tool (GUI) used to manage Cisco ASA security appliances. GUI provides a visual representation of files present and shows live details about systems in infographics. ASDM can be downloaded from Cisco’s website or from ASA’s admin page. ASDM can access the router with its admin username and password. ASDM is convenient at quickly configure, monitor, and troubleshoot Cisco ASAs.

Internet Service Provider (ISP) are organization or companies that provide internet access for its clients. An ISP may also provide other services like webhosting or mailing services. Some common ISP in U.S. includes AT&T, Comcast Xfinity, Time Warner Cable, Verizon and Charter.

Dynamic Host Configuration Protocol (DHCP) is a networking protocol that automatically assigns IP addresses to devices. DHCP provides reliable IP address configuration because it minimizes typographical errors during configuration and provides non-conflicting IP addresses.

Domain Name Service (DNS) transfer name requests into IP addresses. DNS servers are a hierarchy of servers beginning with top domain servers .

Network Address Translation (NAT) translates private IP addresses into public private IP addresses. It is used for slowing down the rate of depletion of available IP address and make IP address allocation easier. Port Address Translation (PAT) translates private IP addresses the public IP address via Port numbers. PAT is much more dynamic than NAT, but NAT is more secure and can be viewed as a superset of PAT

**Lab Summary**

1. Connect the configured switch to the ISP
2. Connect the ASA firewall to the switch
3. Established console connection between pc and the ASA firewall.
4. Console into the firewall with putty from pc.
5. Launch startup wizard and configure ASA

**Lab Commands**

Int – Enter a chosen interface

Nameif – Specify name of an interface

IP address – Set IP address

Switchport access vlan – Issue a vlan to a port

Username password – Set username and password for admin

Http server enable – Enable the HTTPS server

Http – Identify IP address for HTTPS connections

Ip address dhcp setroute – automatically obtain default route

Security-level – Set security level

Dns domain-lookup – Records a list of DNS records

Dns server-group – Create dns server group

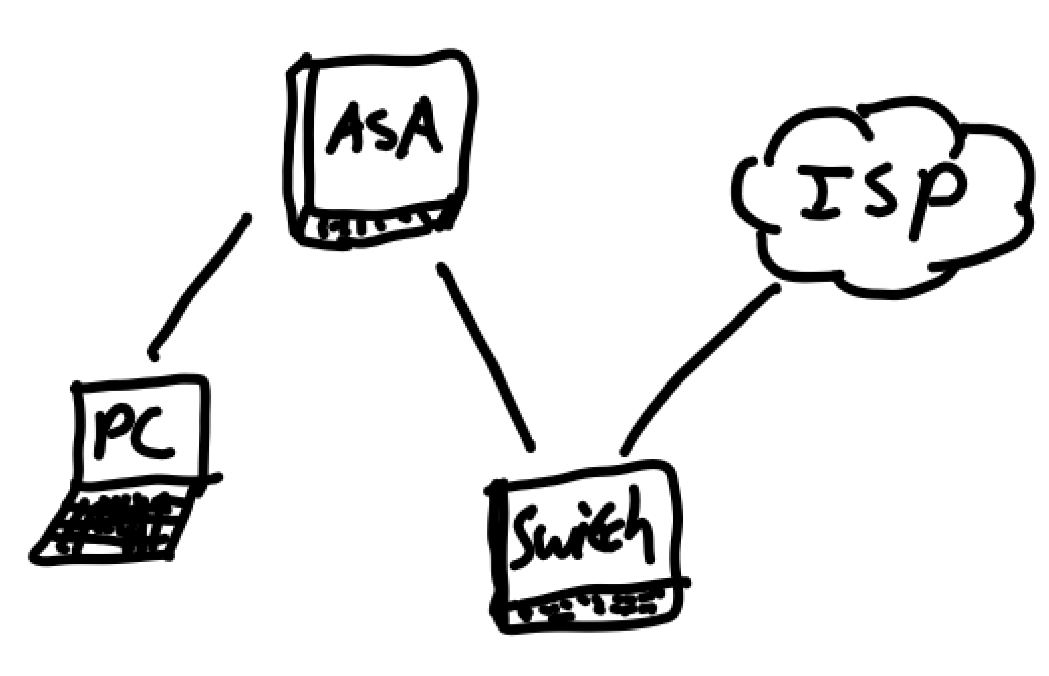
Name-server – Address of server

Dhcpd auto\_config – Set DHCP

Dhcpd address – Set DHCP IP address range

Dhcpd enable – enable DHCP

**Network Diagrams**



**Configuration**

ASA:

*: Saved*

*:*

*: Serial Number: JMX1237Z0B2*

*: Hardware: ASA5505, 1024 MB RAM, CPU Geode 500 MHz*

*:*

*ASA Version 9.2(4)*

*!*

*hostname ciscoasa*

*enable password 8Ry2YjIyt7RRXU24 encrypted*

*names*

*!*

*interface Ethernet0/0*

*switchport access vlan 2*

*!*

*interface Ethernet0/1*

*switchport access vlan 3*

*!*

*interface Ethernet0/2*

*switchport access vlan 3*

*!*

*interface Ethernet0/3*

*switchport access vlan 3*

*!*

*interface Ethernet0/4*

*switchport access vlan 3*

*!*

*interface Ethernet0/5*

*switchport access vlan 3*

*!*

*interface Ethernet0/6*

*switchport access vlan 3*

*!*

*interface Ethernet0/7*

*switchport access vlan 3*

*!*

*interface Vlan1*

*no nameif*

*no security-level*

*no ip address*

*!*

*interface Vlan2*

*nameif outside*

*security-level 0*

*ip address dhcp setroute*

*!*

*interface Vlan3*

*nameif inside*

*security-level 100*

*ip address 192.168.1.1 255.255.255.0*

*!*

*ftp mode passive*

*dns domain-lookup outside*

*dns domain-lookup inside*

*dns server-group DefaultDNS*

*name-server 8.8.8.8*

*object network obj\_any*

*subnet 0.0.0.0 0.0.0.0*

*pager lines 24*

*logging asdm informational*

*mtu outside 1500*

*mtu inside 1500*

*icmp unreachable rate-limit 1 burst-size 1*

*no asdm history enable*

*arp timeout 14400*

*no arp permit-nonconnected*

*!*

*nat (inside,outside) after-auto source dynamic any interface dns*

*timeout xlate 3:00:00*

*timeout pat-xlate 0:00:30*

*timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02*

*timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00*

*timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00*

*timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute*

*timeout tcp-proxy-reassembly 0:01:00*

*timeout floating-conn 0:00:00*

*dynamic-access-policy-record DfltAccessPolicy*

*user-identity default-domain LOCAL*

*http server enable*

*http 192.168.1.0 255.255.255.0 inside*

*no snmp-server location*

*no snmp-server contact*

*crypto ipsec security-association pmtu-aging infinite*

*crypto ca trustpool policy*

*telnet timeout 5*

*no ssh stricthostkeycheck*

*ssh timeout 5*

*ssh key-exchange group dh-group1-sha1*

*console timeout 0*

*dhcpd auto\_config outside*

*!*

*dhcpd address 192.168.1.10-192.168.1.40 inside*

*dhcpd auto\_config outside interface inside*

*dhcpd enable inside*

*!*

*threat-detection basic-threat*

*threat-detection statistics access-list*

*no threat-detection statistics tcp-intercept*

*username cisco password eeH8sl9M4wy/URjZ encrypted*

*!*

*class-map inspection\_default*

*match default-inspection-traffic*

*!*

*!*

*policy-map type inspect dns preset\_dns\_map*

*parameters*

*message-length maximum client auto*

*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*

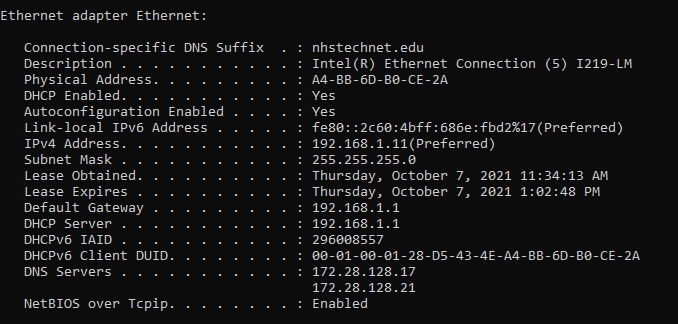
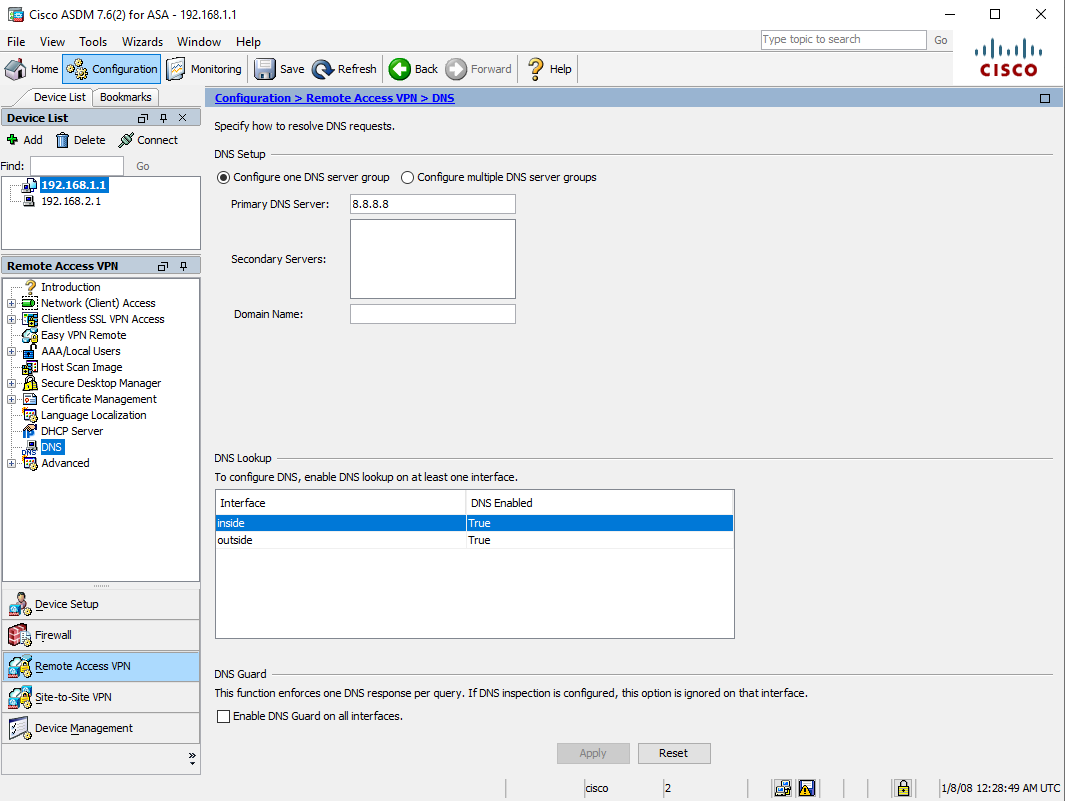
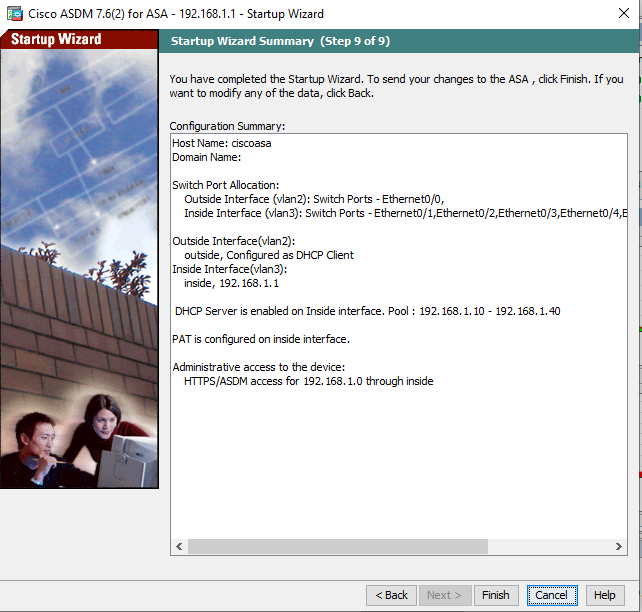
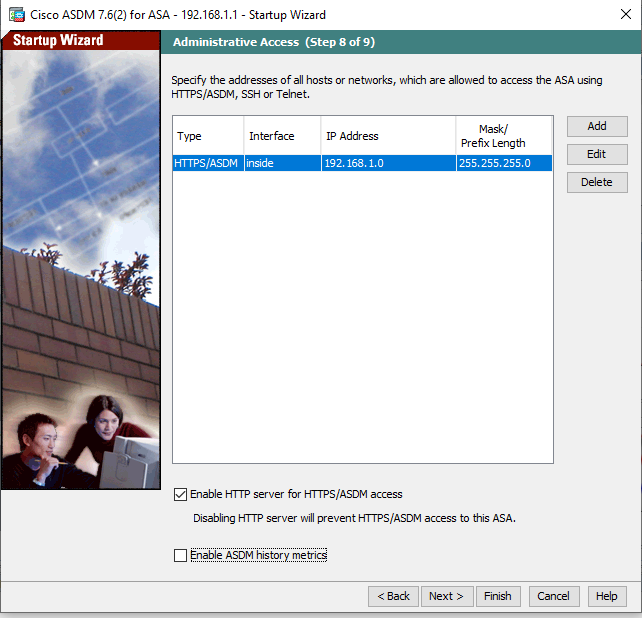
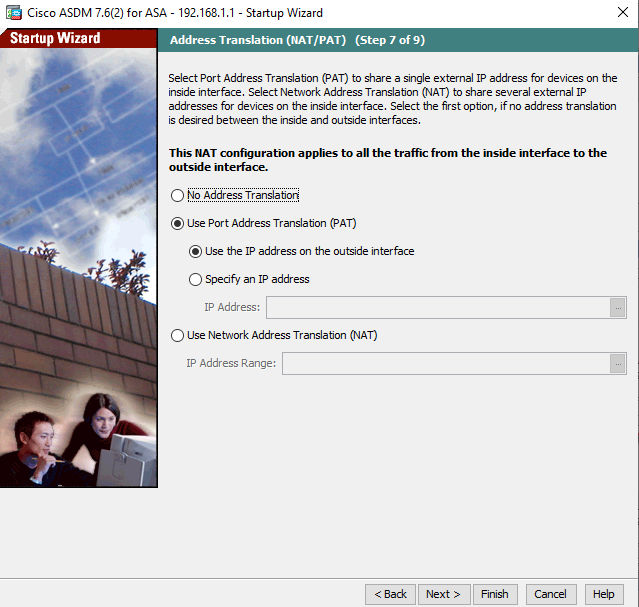
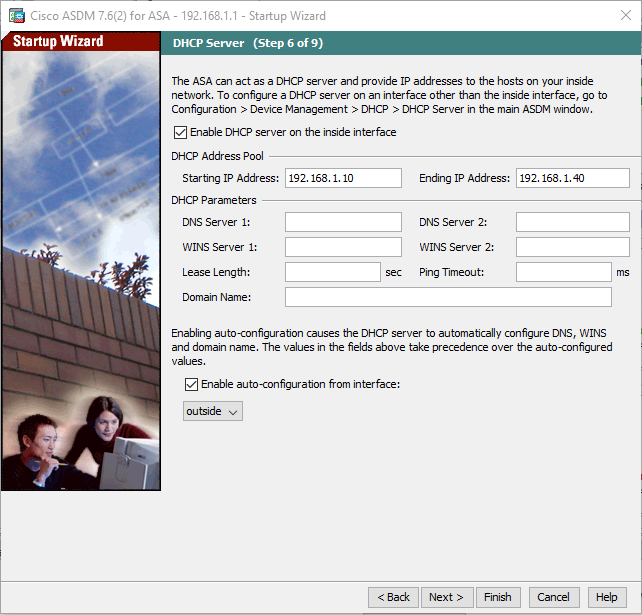
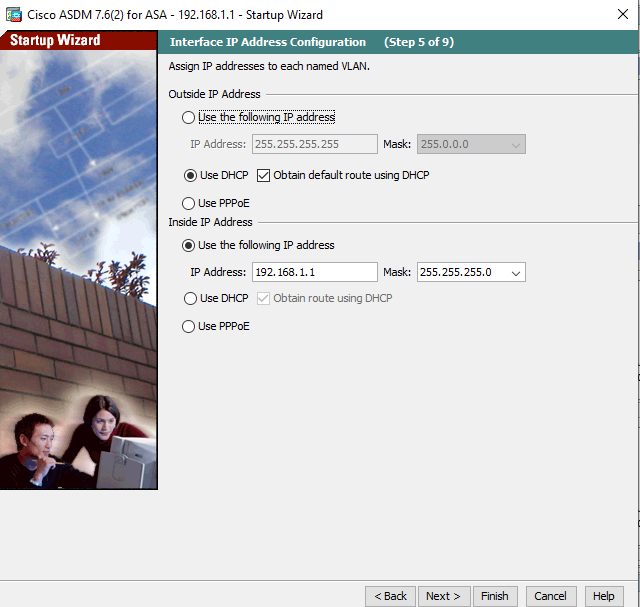
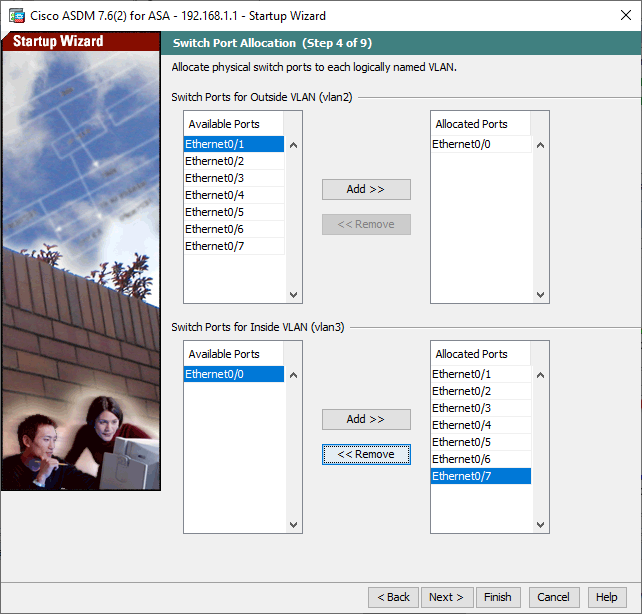
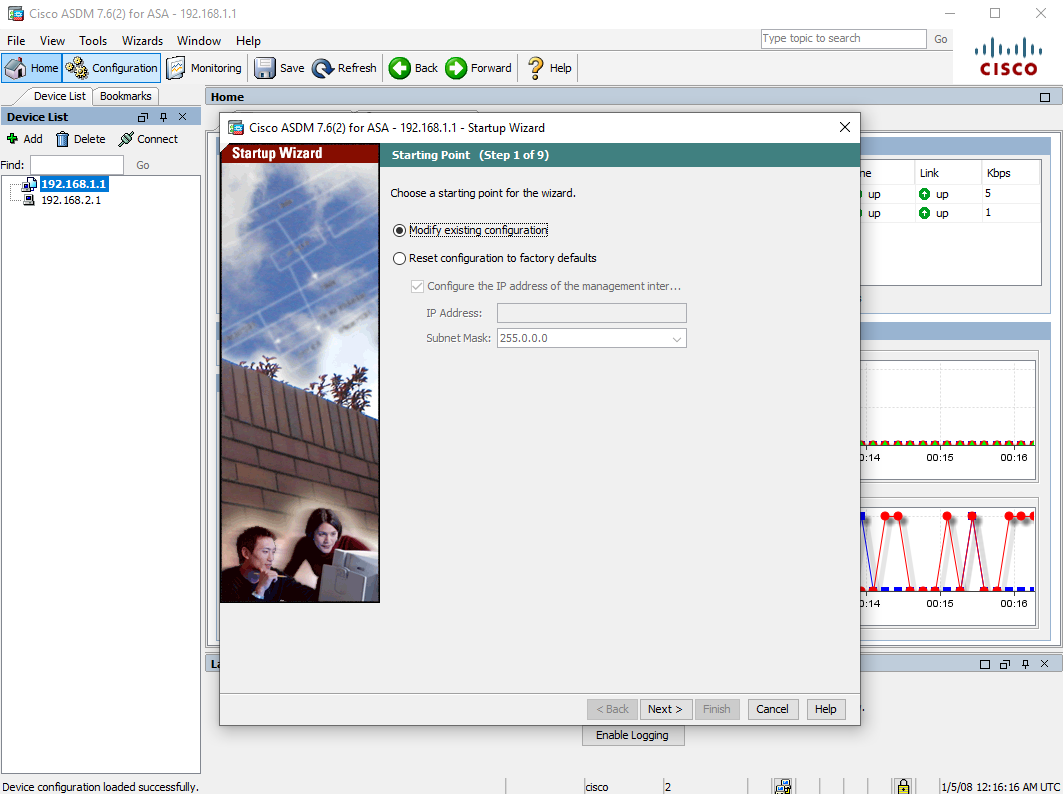
*prompt hostname context*

*call-home reporting anonymous prompt 2*

*Cryptochecksum:2341fc544dfb7efa5f3c3cc139d0cc5f*

*: end*

**Screenshots**



**Problems**

After we ran the startup wizard and configured DHCP, PAT, DNS and IP routes, our PC still could not get the DNS server’s address. We troubleshooted by testing if ASA can get internet connection. We found that ASA can get a public IP address and has a default route set up by DHCP. However, we can’t use ping on ASA because the ASA restricts ping. We later found our issue was caused by an outdated DHCP release. We solved the problem by typing ipconfig/renew command in the pc command prompt.

**Conclusion**

**Diagram, letter

Description automatically generated with medium confidence**In this lab, we configured basic setup on ASA 5505 with Startup Wizard in ASDM. We successfully used the ASA as a default gateway and DHCP server. The DNS server for ASA 5505 and pc was obtained from default route automatically.

**Teacher Signoff**