Firewall Lab

In this lab you will configure firewall rules and apply them to restrict traffic.

STOP: Read all of the material in this week's course material section before attempting this lab. This includes an introduction on Cisco IOS CLI before proceeding.

In this lab you will be asked to configure a router and apply the necessary ACLs to restrict traffic to create various security zones.

Network Topology:

Router interface IP address

Internet-GW Router-

1. Fastethernet 0/1 – 10.11.11.1/24
2. Fastethernet 0/0 – Has to be configured
3. Serial 0/0/1 – 10.1.1.1/24

NEE-FW Router-

1. Fastethernet 0/0 – 10.6.6.1/24
2. Fastethernet 0/1 – 10.7.7.1/24
3. Serial 0/0/1 – 10.1.1.2/30
4. Serial 0/0/0 – 10.2.2.2/30

Home Router-

1. Fastethernet 0/0 – 10.20.20.1/24
2. Serial 0/0/0 – 10.2.2.3/24

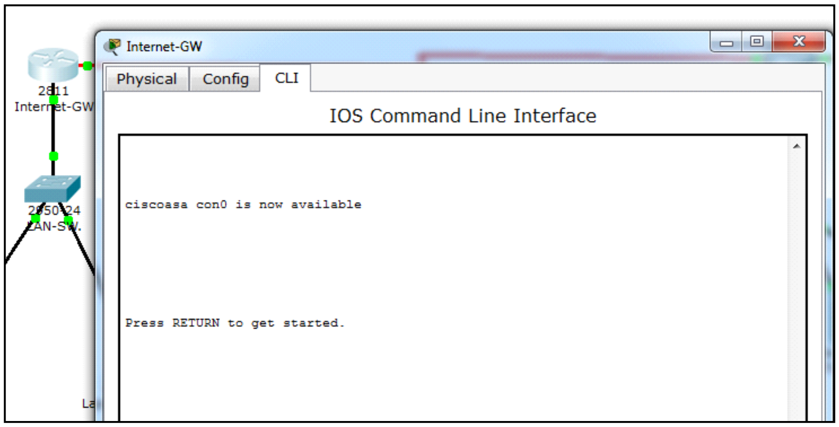
Other IP address can be identified by clicking the device > desktop tab > IP Configuration

Configuring Privilege Access

First, we need to configure the access to the router, in order to prevent unauthorized users with physical access to the device.

The router has two execution modes, user mode or privileged mode. User mode will show the name of the device and '>' as prompt.

- Click on the Internet-GW device and go to the CLI tab

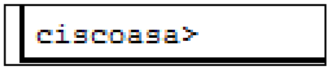


```
ciscoasa con0 is now available



Press RETURN to get started.
```

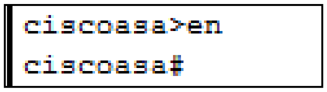
- Hit enter and the user prompt will appear



```
ciscoasa>
```

The user mode has limited commands available and does not allow modifying the configuration of the router. Type **?** to see the available commands.

- To enter privilege mode, type ***enable*** and hit enter



```
ciscoasa>en
ciscoasa#
```

- Now in privileged mode type **?** How has the available commands changed?

- The ***Show*** command has several options that will provide information about the status and configuration of the device. Try the following show commands:

  #show version
  #show flash
  #show ip interface brief

  [Before proceeding answer the following]:
  What version of software is the device running?
  What processor does the device have?
  What is the total memory of the device?
  How much flash space is used vs. available?
  How many and what types of interfaces does the device have?

- Type **show ?** This will show context sensitive help for the command. Try a number of the options to the show command. Did you find anything useful?

- To change the configuration of the router we need to enter **global configuration mode**. Type ***configure terminal or conf t***

- Let's configure a password to the privilege mode, so only authorized users can modify the router's configuration. Type ***enable password ciscopass***

- Test your password settings. Exit the config mode, type ***exit.*** Now, exit the privilege mode by typing ***exit*** again.

- Enter the privilege mode with your newly created password.

- Now, a very important step. All configuration changes are applied to the configuration running on the router's NVRAM. In order to prevent loosing changes whenever the device is restarted, we need to save the running to configuration to startup configuration saved in the router's flash. Type ***copy running-config startup-config***

Configuring Interfaces

Engineering Student's subnet doesn't have connectivity to Internet (Test by opening web browser in Student 1 PC and try to login to **www.neu.edu**). In order to provide connectivity, the interface has to be configured with an IP address.

- Configure the IP address of the interface FastEthernet 0/0, which is connected to the Engineering Student's LAN Switch.
  - First, enter the global config mode. Type ***configure terminal***

  - Enter the interface configuration mode. Type ***interface fastethernet 0/0***

  - Assign an IP address to the interface. Type ***ip address 10.13.13.1 255.255.255.0***

  - Type ***exit*** to return to global config mode

  - Type ***end*** to return to privileged mode

Configuring Services

Configure the Router's (Internet-GW) DHCP to provide dynamic IP address to Student 1 and Student 2.

- Create the DHCP pool. Enter **global config mode** and type ***ip dhcp pool LAN1***

- Define the network for the pool. Because we need the network 10.13.13.0 to receive DHCP, we will assign this network to the DHCP pool. Type ***network 10.13.13.0 255.255.255.0***

- Establish the default router for the network. The DHCP client will receive this parameter as the default gateway in the IP configuration. The IP of the router's internal interface (Fasthethernet 0/0) will be the default gateway. Type ***default-router 10.13.13.1***

- Provide a DNS server for name resolution. The NEU network's DNS server will be the student networks primary DNS. Type ***dns-server 10.7.7.20***

Once the pool is configured we need to exclude some addresses from being leased. Let's limit the scope of the address pool to give out addresses from 10.13.13.100 to 10.13.13.120 only.

- Go back to **global config mode**. Type ***exit***

- Exclude addresses 1 to 99 from the pool. Type ***ip dhcp excluded-address 10.13.13.1 10.13.13.99***

- Exclude addresses 121 to 255 from the pool. Type ***ip dhcp excluded-address 10.13.13.121 10.13.13.255***

- Check the configuration, open Student 1 PC, in the Desktop Tab, Command Prompt, type ***ipconfig*** and verify the PC has received an IP address in the configured range. If not, type ***ipconfig /renew*** and check again. Repeat the same for Student 2 Laptop. Make sure Engineering Student 1 PC and Student 2 Laptop have IP addresses assigned.

  Note: DHCP for CCIS student's subnet has already been configured.

  Try to connect to www.neu.edu from Student 1 and Student 2 web browser. (Wait for few seconds for the page to appear)

- Check connectivity between Internet-GW and NEU network. From the router's console, ***ping*** from privilege mode #
  10.1.1.2
  10.7.7.1
  10.6.6.1

Configuring Remote Access

It is always convenient to have remote access to devices. In this lab we will configure the terminal line to access the router via SSH.

- Generate the RSA key. In **global config mode** type ***crypto key generate rsa***

- Enter the terminal interface configuration mode, ***interface fastethernet 0/0***. In config mode type ***line vty 0 4***

- Define the authentication method. We will use the local user database. Type ***login local***

- Define the protocol allow. Type ***transport input ssh***

- Finally, we need to create a user in the local database. Type ***exit*** to return to config mode. Then type ***username adminssh password adminssh01***

- From the desktop tab in the Engineering PC student 1. Open a command prompt and type **ssh –l adminssh 10.13.13.1**. The SSH connection should establish and it will prompt for user's password. Then, you will see the router's prompt.

Restricting network traffic (ACLs)

Now, we will create ACLs to control the traffic in the student network.

- Test HTTP connectivity to www.neu.edu web server. From the Engineering Student 1 PC and Student 2 Laptop, open a web browser and go to www.neu.edu

- Create an ACL to deny all LAN ---> WAN http traffic. From **global config mode**:

  The ***access-list*** command will give a few options, after each word type ? to see the options. You will see:
  - Type of action to be applied to the traffic (permit, deny, remark)
  - Type of traffic to be matched (ip, icmp, tcp, udp, others)
  - Other options (eq, established, gt, range)

  Type,
  access-list 110 deny tcp any any eq www
  access-list 110 permit ip any any

- Defining the ACL does not enforce it. We need to apply the ACL to an interface. **Refer to the assigned readings** to determine which interface to apply the ACL, as well as the direction of the ACL (inbound or outbound). Enter the **interface configuration mode** and type ***ip access-group 110*** ***{in|out}.***

- Go to Engineering student 1 and browse www.neu.edu site. Is there HTTP connectivity?
- Go to CCIS student 3 and browse www.neu.edu site. Is there HTTP connectivity?

- Remove the ACL with command ***no ip access-group 110 {in|out}*** and try applying the ACL in another direction and/or interface. Do this on all interfaces on Internet-GW router (fastethernet0/0, fastethernet0/1 and serial0/0/1). Which combinations of interface & direction meets the required criteria of blocking HTTP traffic destined from both Engineering and CCIS Student network to WAN host ? **Remember** to remove the ACL before trying a new combination otherwise you will get incorrect results. Decide which is the best interface to apply the ACL.

Review:
In - ACL: source IP is local network, destination is remote
Out - ACL: source IP is remote, destination is local network

[Do not proceed until you have tested the ACL on all Six combinations of Interface/Direction]

In the lab report include which interface and direction was best suited for blocking student network www traffic to the WAN

Save your progress as *lastname-firstname-ia5150.pka*

Default deny statement

Let's change the default action of the security posture. Instead of denying specific traffic and allow everything else, we will allow specific traffic and deny everything else.

- Remove the previously created ACL from the interface. Enter the **interface configuration mode** and type no ip access-group 110 ***{in|out}***

We will create a new ACL with a default deny. For this, we need to establish which traffic we want to allow out of our LAN. Checking the services in the DMZ, identify the protocols needed for basic connectivity. The order of the entries in an ACL is very important, as every statement is matched by the router from top to bottom. Thus, we need to input each rule in the order we want it to match.

Before proceeding verify the e-mail access: Enter the email client of Engineering Student 1 PC and try to send and receive an email to Professor's Laptop

Create **ACL 100** which enforces the following rules:

- Allow ping to work from any host to any host (icmp)
- Allow http traffic from any host to any host (?/?)
- Allow DNS traffic to resolve name queries. (udp/domain)
- Allow DHCP traffic from any host to any host (?/?)
- Deny everything else

Let's apply the ACL to an interface. Entering the interface configuration mode apply the ACL, type ***ip access-group 100 {in|out}***

- Browse the www.neu.edu web site. Is this service allowed?

- Enter the email client of Engineering Student 1 PC and try to send and receive an email to professor. Is this service allowed?

- Ping 10.7.7.10 from Engineering Student 1 PC? Is this service allowed

[DO NOT Proceed until ACL is enforcing default deny. Mail should not be functional]

- From the privilege mode #, type ***show access-lists***, see what rules have been matched so far.

Targeted ACL

Now, let's create a more specific ACL, in order to block traffic from the student network

- Remove the previously ACL from the interface. Enter the interface configuration mode and type **no ip access-group 100** {in|out}

- Type show ***running-config*** to see the current configuration. Copy and paste your previously created ACL 100 to a Notepad document. In Notepad change the all **access-list IDs from 100 to 120**

- In your Notepad document insert a new line at the **beginning** of the ACL. This ACE (access control entry) should ***deny*** access to ***WWW*** service from CCIS students subnet to ***host*** *www.eng*.neu.edu.

- Next insert a new line at the beginning of ACL, This ACE should ***deny*** access to ***WWW*** for engineering students' subnet to the host *www.ccis.neu.edu.* This is a subnet targeted ACL and should be as specific as possible. Ensure that both the department students are able to access www.neu.edu.

- Next insert two new lines at the **beginning** of the ACL to allow mail service. These two ACEs (access control entries) should ONLY ***allow*** access to ***mail (SMTP and POP3)*** service from ***CCIS Student Network***.

- Copy and Paste the modified ACL to your router's console. Apply ACL 120 to the proper interface in the proper direction as you did previously with ACLs in the lab.

- Verify that CCIS students can't access www.eng.neu.edu server and engineering students can't access www.ccis.neu.edu server. Also, verify that both are permitted to browse to www.neu.edu. Enter the email client in CCIS student PC and send an email to hruser. Send a mail from Engineering student PC to hruser and see if it is blocked. (hruser@neu.edu)

Hint: 4 ACEs should be added in front of the ACL created in previous section.

At this point your Activity wizard will show 100% completion.

Save your router configuration to the startup-config (. Save the packet tracer file to lastname-firstname-ia5150.pka and submit to blackboard.

Bonus (10%)

Secure the environment

Internet-GW Router:

- Recreate your SSH key, use 2048 bit encryption with only SSH v2.0
- Create static ARP entries for each server or laptop. Verify they function correctly
- Create ACL and limit access to SSH to the Internet-GW router to only Student2-PC and apply it to the correct interfaces to limit access. Verify Functionally.

Provide Screen Shots and explanation wherever possible.

Bonus (additional 10%)

Configure the Home router of the professor to connect to a site-to-site VPN in order to securely access the finance server from professor's home network. Use the following parameters:

Pre share key: netseclab
Transform set: esp-aes and esp-sha-hmac

After configuring the VPN. Type **configure terminal** and type **do show crypto isakmp sa.**

Take screen shot of the result and submit it along with the report. Also, Include and explain your configuration in the report.