INFO8490 Lab 6 Packet Filtering Firewall

Overview

This Lab will be recorded in your lab book and requires you to configure packet filtering firewalls. You will gain practical experience configuring packet filtering. This type of configuration is common on border routers assuming there are no extensive firewall functions on the edge device (i.e. there is a firewall with more capability behind the edge device).

Remember you must follow all standard naming conventions (including when name Access Control Lists)

Read through the entire lab first so that you completely understand what you are trying to achieve and create a basic plan. This will likely save you problems and having to repeat work later on.

Please note that this Lab is an individual activity you will not be sharing your network devices or work.

Preparation

You will need:

1. The most current version of Packet Tracer
2. The packet tracer file that you created in Lab 4
3. You will use the IP addresses assigned to you in Lab 4.
4. All passwords must be Secret55

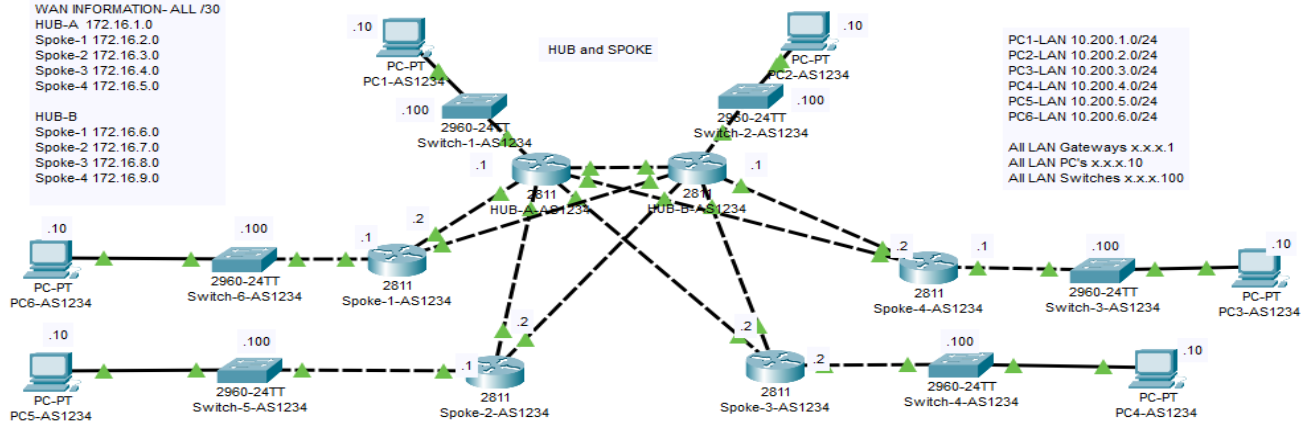
Description

This lab expects that you have fully completed the requirements for Lab 1through 5. In Lab 6 you will be adding IP security to the topology deployed in lab 4 (See Figure 1-1). You will configure or reconfigure the networking devices and hosts as necessary. You will be submitting only one packet tracer file for this LAB. Make sure that each part is complete and functioning before you move on to the next part,

In your own words, provide a description of the expected goals and results as you understand them to be.

Lab Schematic **(this is my example, please create your own schematic)**

Figure 1-1 Topology f



or

Stateless Packet Filtering

***Be sure that all Network and naming information is provided in the schematic in packet tracer.**

Part 1 – Initial Configuration of the Topology (Assumes that you have completed the following on all network devices)

1. Configure the Privileged Mode Password
2. Enforcing Login
3. Configure Telnet and Secure Shell
4. Configuring IP Addresses
5. Configure routing

Test your initial configuration

1. Each PC can communicate with all other PC's

Save the packet tracer file and the running config to startup config.

Screenshots

Although the No screenshots are necessary for Part 1, those steps must be completed before moving on.

Part 2 - Configure Standard Access Lists

Description

In your own words, provide a description of the expected goals and results as you understand them.

Create Standard ACL

You will configure simple packet filtering in this part. The goal in our topology is to allow the hosts in spoke 1 and spoke 2 to communicate with hosts on all other spokes but not with each other. There will not be any traffic that is not defined below.

Using your topology from Part 1-6, configure as follows:

1. On Spoke-1:
   - 1.1. Create and name a standard access list that
     - 1.1.1. Denies traffic from the LAN networks on Spoke-2 and Spoke-4
     - 1.1.2. Allows traffic from any other network
   - 1.2. Apply that access list inbound on the external interfaces on Spoke-1
2. On Spoke-2:
   - 2.1. Create and name a standard access list that
     - 2.1.1.Denies traffic from the LAN networks on Spoke-1 and Spoke 4
     - 2.1.2.Allows traffic from any other network
   - 2.2. Apply that access list inbound on the external interfaces on Spoke-2
3. Test your access lists
   - 3.1. Ensure that all other PC's can communicate with the PC's on Spoke-1, Spoke-2 and Spoke-4
   - 3.2. Ensure PC's on Spoke-1 and Spoke-2 cannot communicate with each other
   - 3.3. Ensure that the PC on Spoke-4 cannot communicate the PC's on Spoke-1 and Spoke-2

Now Remove the ACE from each Spoke that Allows Traffic from "any" other network. Rerun the tests above, write and detailed explanation of the results, be sure to explain what happens and why.

****Be sure to put the ACE back in your ACLs*****

Screenshots

Include a screenshot of:

1. Each Spoke using a command (not sh run) to show the ACL name, any ACE's and any filtering caused by the ACLs.
2. Each Spoke showing which interfaces the access-lists are assigned to.
3. Each step involved in testing your access lists as outlined in step 3 above.

Observations

Record your observations including details on any problems encountered or solved.

Reflection

Write a reflection about this part of the lab. Discuss things like: the path the ping traffic takes from the one spoke to another, where that traffic stops, and why; how you would modify the packet filtering configuration using standard access lists to achieve the same effect but configured on spoke-4 rather than Spoke-1 and Spoke-2. (try configuring it). Also, be sure to reflect on what happened when you removed the ACE to allow any source, why did this happen? Record any additional reflections based on your observations and problems you encountered.

Wrap Up

Remember to save your Packet Tracer File (You will be using the same file in Part 3)

Part 3 - Configure Extended Access Control Lists

Preparation

In addition to the topology, you will continue using the same packet tracer file and configuration completed in Parts 1 and 2. Do not remove the ACL's that you created in Part 2.

Description

You will configure more complex packet filtering in this part. The goal in our topology is to allow the users in the LAN connected to HUB A and HUB B to access hosts in all other LAN's while network hosts on other LANS will access only specific ports on HUBs A and B. Telnet traffic will only be permitted from the PC's connected to Spokes 1-3 from the LAN interface on HUB A. SSH traffic will only be permitted from the PC's connected to Spokes 4-6 to the LAN Interface on HUB B. Ping traffic will be allowed from all sites.

Note that we will be using telnet and ssh from the PC's to the LAN interfaces on the routers rather than to the actual workstations. Unfortunately Packet Tracer doesn't support Telnet/SSH to PC/Server objects. With that said, the same principles still apply.

In your own words, provide a description of the expected goals and results as you understand them.

Create Extended ACL

You can use the topology settings you saved from Parts 1 and 2. Remember that you must be specific. You must be able to differentiate between LAN interface, Hosts and Networks when configuring access control entries. You will lose marks for ambiguous entries. There will not be any traffic that is not defined below.

Configure as follows:

1. On HUB A:
   1.1. Create and name an extended access list.
   1.2. Add a rule to the extended access list that allows EIGRP traffic from any network. Make the rule as specific as possible.
   1.3. Add a rule to the extended access list that allows ping traffic from any host on HUB B LAN, Spoke-1 and spoke 2 to the PC on HUB A. Make the rule as specific as possible.
   1.4. Add a rule to the extended access list that allows telnet traffic from the PC (Host) on HUB B as well as Spokes 1 and 2 to the LAN on HUB A. Make the rule as specific as possible.
   1.5. Add a rule that denies all other traffic
   1.6. Apply that access list inbound on to each of the external (WAN) interfaces connecting to HUB A.

2. On HUB B:
   2.1. Create and name an extended access list.
   2.2. Add a rule to the extended access list that allows EIGRP traffic from any network. Make the rule as specific as possible.
   2.3. Add a rule to the extended access list that allows ping traffic from any host on HUB A LAN, Spoke-3 and spoke-4 to the PC on HUB B. Make the rule as specific as possible.
   2.4. Add a rule to the extended access list that allows SSH traffic from the PC (Host) on HUB A as well as Spoke-3 and Spoke-4 to the LAN on HUB B. Make the rule as specific as possible.
   2.5. Add a rule that denies all other traffic
   2.6. Apply that access list inbound on to each of the external (WAN) interfaces connecting to HUB B.

3. Test your access lists
   3.1. Ensure that only PC's on the LAN's defined in your access lists can ping the PC's on HUB A and HUB B LANS as required.
   3.2. Ensure that only the PC's on Spokes 1 and 2 can telnet into the HUB A LAN interface.
   3.3. Ensure that only the PC's on Spokes 3 and 4 can SSH into the HUB B LAN interface.
   3.4. Ensure that no other traffic is permitted

Screenshots

Include a screenshot of:

1. Each HUB using a command (not sh run) to show the ACL name, any ACE's and any filtering caused by the ACLs.
2. Each HUB showing which interfaces the access-lists are assigned to.
3. Each step involved in testing your access lists as outlined in step 3 above.

Observations

Record your observations including details on any problems encountered or solved.

Reflection

In your own words provide a detailed explanation of what each of the ACE's mean and how they are affecting network traffic. Describe what would happen (and why) if you tried to telnet from PC4 to the LAN on HUB B or SSH from PC6 to the LAN on HUBA. Also explain the benefit of using extended access lists over standard access lists. Be sure to record and additional reflections and solutions to problems that you encountered.

Wrap Up

Remember to save your Packet Tracer File