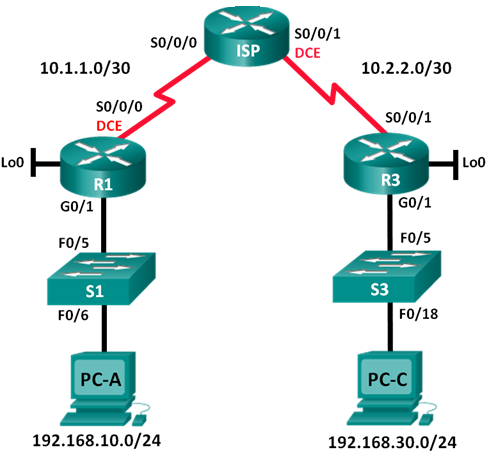
Lab 4 – Configuring and Verifying Extended ACLs

1. Student No: Name:

**See bottom of this page for Instructions.**

1. Topology



**G0/1**

**G0/0**

**192.168.10.3**

**192.168.30.3**

**209.165.201.0/27**

**192.168.30.0/24**

**192.168.10.0/24**

**209.165.200.224/27**

**209.165.201.2**

**209.165.200.226**

**192.168.20.1**

**INSTRUCTIONS**

**Answer the questions marked in Red as you do the Lab**

**Download this Lab doc. Save it with your student number in the filename.**

**Download the Packet Tracer File. Save it with your student number in the filename.**

**Type your answers to the questions into this Lab doc.**

**Put completed Lab doc AND Packet Tracer File in one Zip file.**

**Upload the Zip to Bright Space at end of Lab today.**

**192.168.40.1**

1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| R1 | G0/1 | 192.168.10.1 | 255.255.255.0 | N/A |
|  | Lo0 | 192.168.20.1 | 255.255.255.0 | N/A |
|  | S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A |
| ISP | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
|  | S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A |
|  | G0/1 | 209.165.201.1 | 255.255.255.224 | N/A |
|  | G0/0 | 209.165.200.225 | 255.255.255.224 | N/A |
| R3 | G0/1 | 192.168.30.1 | 255.255.255.0 | N/A |
|  | Lo0 | 192.168.40.1 | 255.255.255.0 | N/A |
|  | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| Web-1 | NIC | 209.165.201.2 | 255.255.255.224 | 209.165.201.1 |
| Web-2 | NIC | 209.165.200.226 | 255.255.255.224 | 209.165.200.225 |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-C | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |

1. Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

* Configure basic settings on PCs, routers, and web servers.
* Configure OSPF routing on R1, ISP, and R3.

Part 3: Configure and Verify Extended Numbered and Named ACLs

* Configure, apply, and verify a numbered extended ACL.
* Configure, apply, and verify a named extended ACL.

1. Background / Scenario

Extended access control lists (ACLs) are extremely powerful. They offer a much greater degree of control than standard ACLs as to the types of traffic that can be filtered, as well as where the traffic originated and where it is going.

In this lab, you will set up filtering rules for two offices represented by R1 and R3. Management has established some access policies between the LANs located at R1 and R3, which you must implement. The ISP router between R1 and R3 does not have any ACLs placed on it. You would not be allowed any administrative access to an ISP router as you can only control and manage your own equipment.

1. Required Resources – Already set up in the clean Packet Tracer file provided.

* Use 3 x Cisco 1941 Routers in PT.
* 2 x Cisco 2960 Switches.
* 2 x Servers (Packet Tracer Server-PT End Devices) – Web-1 and Web-2.
* 2 PCs (Packet Tracer PC-PT End Devices) –PC-A and PC-C

1. Set Up the Topology and Initialize Devices - Already set up.

In Part 1, you will create the network topology. Already created.

* 1. Cable the network as shown in the topology. Already done.

1. Configure Devices and Verify Connectivity

In Part 2, you will configure basic settings on the routers and PCs. Refer to the Topology and Addressing Table for device names and address information. You have been provided with the basic device settings in the Part-2-Base-configs.txt file. Paste in the configs for Steps 1 to 4 from this file to config the basic settings.

* 1. Configure IP addresses on Web-1, Web-2, PC-A and PC-C.
  2. Configure basic settings on R1.
     1. Disable DNS lookup, i.e. configure **no ip domain-lookup.**
     2. Configure the device name as shown in the topology.
     3. Create a loopback interface on R1.
     4. Configure interface IP addresses as shown in the Topology and Addressing Table.
     5. Assign a clock rate of **128000** to the S0/0/0 interface.
     6. .Configure **logging synchronous** for the console line.
  3. Configure basic settings on ISP.
     1. Configure the device name as shown in the topology.
     2. Create the loopback interfaces on ISP.
     3. Configure interface IP addresses as shown in the Topology and Addressing Table.
     4. Disable DNS lookup.
     5. Assign a clock rate of **128000** to the S0/0/1 interface.
     6. Configure **logging synchronous** for console line.
  4. Configure basic settings on R3.
     1. Configure the device name as shown in the topology.
     2. Create a loopback interface on R3.
     3. Configure interface IP addresses as shown in the Topology and Addressing Table.
     4. Disable DNS lookup.
     5. Configure **logging synchronous** on the console line.
  5. Configure OSPF routing on R1, ISP, and R3.
     1. Assign 1 as the OSPF process ID and advertise all networks on R1, ISP, and R3. The OSPF configuration for R1 and R2 is included for reference. You must work out the OSPF configs for R3 yourself.
     2. R1(config)# **router ospf 1**

R1(config-router)# **network 192.168.10.0 0.0.0.255 area 0**

R1(config-router)# **network 192.168.20.0 0.0.0.255 area 0**

R1(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

* + 1. ISP (config)# **router ospf 1**

ISP(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

ISP(config-router)# **network 10.2.2.0 0.0.0.3 area 0**

ISP(config-router)# **network 209.165.200.224 0.0.0.31 area 0**

ISP(config-router)# **network 209.165.201.0 0.0.0.31 area 0**

* + 1. After configuring OSPF on R1, ISP, and R3, verify that all routers have complete routing tables listing **all** networks. Troubleshoot if this is not the case.
  1. Verify connectivity between devices.

**Note**: It is very important to verify connectivity **before** you configure and apply ACLs! Ensure that your network is properly functioning before you start to filter out traffic.

* + 1. From PC-A, ping PC-C and the loopback and serial interfaces on R3.

Were your pings successful? YES

* + 1. From R1, ping PC-C and the loopback and serial interface on R3.

Were your pings successful? YES

* + 1. From PC-C, ping PC-A and the loopback and serial interface on R1.

Were your pings successful? YES

* + 1. From R3, ping PC-A and the loopback and serial interface on R1.

Were your pings successful? YES

* + 1. From PC-A, ping the G0/0 and G0/1 interfaces on the ISP router.

Were your pings successful? YES

* + 1. From PC-C, ping the G0/0 and G0/1 interfaces on the ISP router.

Were your pings successful? YES

* + 1. Open a web browser on PC-A and go to <http://209.165.201.2> You should see Webpage from Web-1 server.
    2. Open a web browser on PC-C and go to <http://209.165.200.226> You should see Webpage from Web-2 server.

1. Configure and Verify Extended Numbered and Named ACLs

Extended ACLs can filter traffic in many different ways. Extended ACLs can filter on source IP addresses, source ports, destination IP addresses, destination ports, as well as various protocols and services.

The security policies you are to implement are as follows:

1. Allow web traffic from the 192.168.10.0/24 network to go to any network.
2. Block web traffic from the 192.168.30.0/24 network from accessing Web-2 host. Allow web traffic from 192.168.30.0/24 network to access the 209.165.201.0 network.

A best practice is to place extended ACLs as close to the source as possible. We will follow this practice for these policies.

* 1. Configure a numbered extended ACL on R1 for security policy number 1.

You will use a numbered extended ACL on R1. What are the ranges for extended ACLs?

* + 1. Configure the ACL on R1. Use 100 for the ACL number.

R1(config)# **access-list 100 remark Allow Web Access**

R1(config)# **access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 80**

What does the 80 signify in the command output listed above?

HTTP PORT

To what interface should ACL 100 be applied?

S0/0/0

In what direction should ACL 100 be applied?

OUT

* + 1. Apply ACL 100 to the S0/0/0 interface.

R1(config)# **interface s0/0/0**

R1(config-if)# **ip access-group 100 out**

* + 1. Verify ACL 100.
       1. Open up a web browser on PC-A, and access <http://209.165.201.2> (Web-1). It should be successful; troubleshoot, if not.
       2. From privileged EXEC mode prompt on R1, issue the **show access-lists** command.

R1# **show access-lists**

Note that the Router keeps track of the matches.

Extended IP access list 100

10 permit tcp 192.168.10.0 0.0.0.255 any eq www (10 match(es)

3) From the PC-A command prompt, issue a ping to Web-1’s IP address 209.165.201.2

Explain your results.

UNSUCCESSFUL PING DUE TO IP TRAFFIC BEING BLOCKED

* 1. Configure a named extended ACL on R3 for security policy number 2.
     1. Configure the policy on R3. Name the ACL WEB-POLICY.

R3(config)# **ip access-list extended WEB-POLICY**

R3(config-ext-nacl)# **deny tcp 192.168.30.0 0.0.0.255 host 209.165.200.226 eq 80**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 209.165.201.0 0.0.0.31 eq 80**

* + 1. Apply ACL WEB-POLICY to the S0/0/1 interface.

R3(config-ext-nacl)# **interface S0/0/1**

R3(config-if)# **ip access-group WEB-POLICY out**

* + 1. Verify the ACL WEB-POLICY.
       1. From R3 privileged EXEC mode command prompt, issue the **show ip interface s0/0/1** command.

What, if any, is the name of the ACL? THE WEB-POLICY

In what direction is the ACL applied? OUT

* + - 1. Open up a web browser on PC-C and access <http://209.165.201.2> web page (Web-1). It should be successful; troubleshoot, if not.
      2. From PC-C, open a web session to <http://209.165.200.226> web page on (Web-2). It should fail; troubleshoot, if not.
      3. From a PC-C command prompt, ping PC-A. What was your result and why?

IP TRAFFIC IS NOT PERMITTED THEREFORE IT WAS UNREACHABLE

1. Reflection
   1. Why is careful planning and testing of ACLs required?

TO ENSURE THE NETWORK IS SAFE AND RELIABLE

* 1. Which type of ACL is better: standard or extended?

THERE IS MANY MORE FUNCTIONALITIES AND USES TO EXTENDED THEREFORE IT IS BETER, HOWEVER STANDARD IS ALSO GOOD WITH ITS SIMPLICITY

1. Router Interface Summary Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Router Interface Summary | | | | |
| Router Model | Ethernet Interface #1 | Ethernet Interface #2 | Serial Interface #1 | Serial Interface #2 |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| **Note**: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface. | | | | |