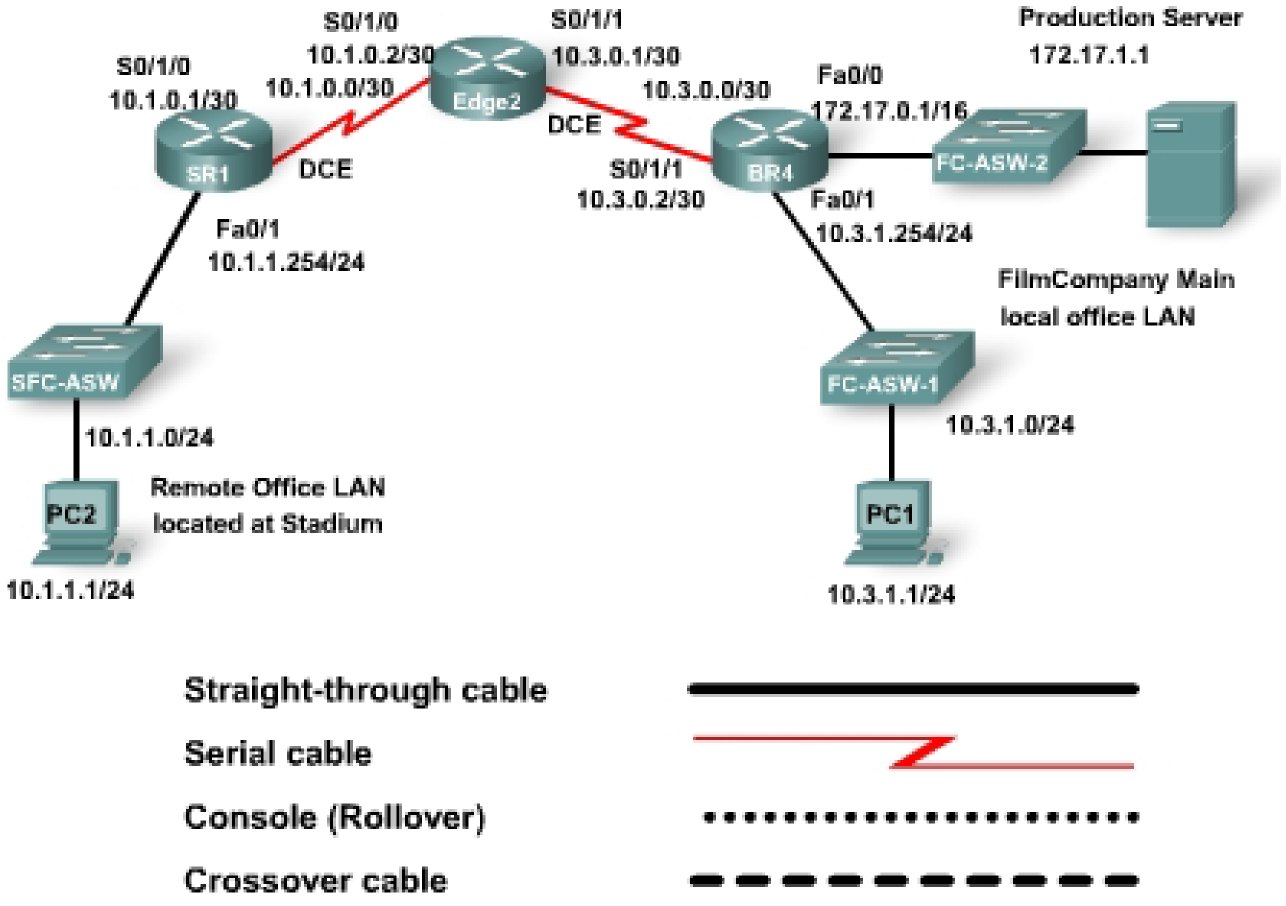
Lab 5.5.3 Developing ACLs to Implement Firewall Rule Sets



Device	Interface	IP Address
SFC-ASW	VLAN 1	10.1.1.253/24
SR1	Fa0/1 S0/1/0	10.1.1.254/24 10.1.0.1/30
Edge2	S0/1/0 S0/1/1	10.1.0.2/30 10.3.0.1/30
BR4	S0/1/1 Fa0/0 Fa0/1	10.3.0.2/30 172.17.0.1/16 10.3.1.254/24
FC-ASW-2	VLAN 1	172.17.1.25/16
FC-ASW-1	VLAN 1	10.3.1.253/24
PC1	—	10.1.1.1/24
PC2	—	10.3.1.1/24
Production Server	—	172.17.1.1/16

Objectives

- Interpret a security policy to define firewall rules.
- Create ACL statements to implement firewall rules.
- Configure and test ACLs.

640-802 CCNA Exam Objectives

This lab contains skills that relate to the following CCNA exam objectives:

- Describe the purpose and types of ACLs.
- Configure and apply ACLs based on network filtering requirements, including CLI/SDM.
- Configure and apply ACLs to limit Telnet and SSH access to the router using SDM/CLI.
- Verify and monitor ACLs in a network environment.
- Troubleshoot ACL issues.

Expected Results and Success Criteria

Before starting this lab, read through the tasks that you are expected to perform. What do you expect the result of performing these tasks will be?

____

____

____

What are the inherent risks of not using an ACL to secure network traffic?

____

____

____

What are several methods to limit the flow of traffic in to and out of LANs or WANs?

____

____

____

Background / Preparation

The FilmCompany provides services to branch offices such as the one located at the stadium. This office has some minor security and performance concerns. These concerns will require the network designer to incorporate several ACLs to secure the network. The ACLs need to be implemented as a simple and effective tool to control traffic.

Given a security policy for the FilmCompany, create a firewall rule set and implement Named Extended ACLs to enforce the rule set.

The security policy for the FilmCompany has a section that relates to access from remote sites. Here is the text from the security policy:

Security Policy

Users accessing the network from remote locations, including remote branch offices, require the following access to the on-site network resources:

1. Remote users must be able to access the Production Server in order to view their schedules over the web and to enter new orders.
2. Remote users must be able to FTP files to and from the Production Server.
3. Remote users can use the Production Server to send and retrieve email using IMAP and SMTP protocols.
4. Remote users must not be able to access any other services available on the Production Server.
5. No traffic is permitted from individual workstations at the main office to remote worker workstations. Any files that need to be transferred between the two sites must be stored on the Production Server and retrieved via FTP.
6. No traffic is permitted from workstations at the remote site to workstations at the main site.
7. No Telnet traffic is permitted from the remote site workstations to any devices, except their local switch.

Step 1: Cable and connect the network as shown in the topology diagram

NOTE: If the PCs used in this lab are also connected to your Academy LAN or to the Internet, ensure that you record the cable connections and TCP/IP settings so that these can be restored at the conclusion of the lab.

a. Connect and configure the devices in accordance with the given topology and configuration.

   Routing will have to be configured across the serial links to establish data communications.

   NOTE: Your instructor may substitute for Production Server an equivalent server for this lab.

b. Configure Telnet access on each router.

c. Ping between Host1, Host2, and Production Server to confirm network connectivity.

   Troubleshoot and establish connectivity if the pings or Telnet fail.

Step 2: Perform basic router configurations

a. Configure the network devices according to the following guidelines:

   - Configure the hostnames on each device.
   - Configure an EXEC mode password of **class.**

- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.
- Configure IP addresses on all devices.
- Enable EIGRP on all routers and configure each to advertise all of the connected networks.
- Verify full IP connectivity using the **`ping`** command.

b. Confirm Application Layer connectivity by telneting to all routers.

Step 3: Create firewall rule set and access list statements

Using the security policy information for the FilmCompany remote access, create the firewall rules that must be implemented to enforce the policy. After the firewall rule is documented, create the access list statement that will implement the firewall rule. There may be more than one statement necessary to implement a rule.

An example of one of the firewall rules is shown:

Security Policy 1: Remote users must be able to access the Production Server to view their schedules over the web and to enter new orders.

Firewall Rule: Permit users on the 10.1.1.0/24 access to the Production Server (172.17.1.1) on TCP port 80.

Access List statement(s): `permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 80`

Access List placement: Inbound on router SR1 Fa0/1 (remember that extended ACLs should be placed close as possible to the source of the traffic)

For each of the following security policies:

a. Create a firewall rule.

b. Create an access list statement.

c. Determine the access list placement to implement the firewall rule.

Security Policy 2: Remote users must be able to FTP files to and from the Production Server.

Firewall Rule:

____

____

Access List statement(s):

____

____

Access List placement:

____

____

Security Policy 3: Remote users can use the Production Server to send and retrieve email using IMAP and SMTP protocols.

Firewall Rule:

Access List statement(s):

Access List placement:

Security Policy 4: Remote users must not be able to access any other services available on the Production Server.

Firewall Rule:

Access List statement(s):

Access List placement:

Security Policy 5: No traffic is permitted from individual workstations at the main office to remote worker workstations. Any files that need to be transferred between the two sites must be stored on the Production Server and retrieved via FTP.

Firewall Rule:

Access List statement(s):

Access List placement:

Security Policy 6: No traffic is permitted from workstations at the remote site to workstations at the main site.

Firewall Rule:

Access List statement(s):

____

____

Access List placement:

____

____

Security Policy 7: No Telnet traffic is permitted from the remote site workstations to any devices, except their local switch.

Firewall Rule:

____

____

Access List statement(s):

____

____

Access List placement:

____

____

Step 4: Create Extended ACLs

a. Review the access list placement information that you created to implement each of the FilmCompany security policies. List all of the different access list placements that you noted above.

____

____

____

Based on the placement information, how many access lists do you have to create?

On Router SR1 _______________

On Router Edge2 ______________

On Router BR4 ________________

b. Based on the access list statements you developed in Task 3, create each access list that is needed to implement the security policies. When creating access lists, remember the following principles:

- Only one access list can be applied per protocol, per direction on each interface.
- Access list statements are processed in order.
- Once an access list is created and applied on an interface, all traffic that does not match any access list statement will be dropped.

c. Use a text file to create the access lists, or write them here. Evaluate each access list statement to ensure that it will filter traffic as intended.

____

____

____

____

____

____

____

____

____

____

____

____

Why is the order of access list statements so important?

____

____

____

Step 5: Configure and test access lists

a. Configure the access lists on the appropriate routers and apply them to the correct interfaces. Name the access lists with representative names, like “RemoteOffice” or “FilterRemote.”

Access list names:

____

____

b. Test the access lists and their placement by performing the following tests:

1) Using Host1, open a browser and attempt to view a web page located on the Production server using the http://172.17.1.1 address.

Were you successful? __________

2) Using Host1, open a browser and attempt to connect to the Production server using ftp://172.17.1.1.

Were you successful? __________

3) Using Host1, attempt to Telnet to any address on any of the routers or switches.

Were you successful? __________

4) Using Host1, attempt to ping Host2.

Were you successful? __________

5) Using Host2, attempt to ping Host1.

Were you successful? __________

Did your ACLs perform as you expected? __________

If not, correct and retest the ACLs and their placement within the network.

Step 6: Document the router configurations

Copy and save the running-configuration outputs from all routers into a word processing document to view their configurations.

Step 7: Reflection

The design strategies for the FilmCompany LAN pose many challenges for the designer. What were a few of the more difficult challenges of creating an ACL you encountered?

____

____

____

____

Consider and discuss the identified strategies. Do all of the strategies designed or hardware identified accomplish the task the same way?

____

____

Would one ACL work better than another?

____

____

Would the chosen ACL design allow for future growth and the addition of more hosts on the LAN segment?

____

____