FTP Denied

Objective

Implement packet filtering using extended IPv4 ACLs according to networking requirements (to include named and numbered ACLs).

Scenario

It was recently reported that viruses are on the rise within your small- to medium-sized business network. Your network administrator has been tracking network performance and has determined that one particular host is constantly downloading files from a remote FTP server. This host just may be the virus source perpetuating throughout the network!

Use Packet Tracer to complete this activity. Write a named ACL to deny the host access to the FTP server. Apply the ACL to the most effective interface on the router.

To complete the physical topology, you must use:

- One PC host station
- Two switches
- One Cisco 1941 series Integrated Services Router
- One server

Using the Packet Tracer text tool, record the ACL you prepared. Validate that the ACL works to deny access to the FTP server by trying to access the FTP server's address. Observe what happens while in simulation mode.

Save your file and be prepared to share it with another student, or with the entire class.

Reflection

1. What was the most difficult part of completing this modeling activity?

2. How often do you think network administrators need to change their ACLs on their networks?

3. Why would you consider using a named extended ACL instead of a regular extended ACL?