

Real-World Scenario 8-1: Access Control Lists

Scenario: You are tasked with blocking both DNS requests and zone transfers coming from outside IP addresses. Your organization uses a firewall configured with an implicit allow. Also, the following ACL is applied to its external interface:

Permit TCP ANY ANY 80

Permit TCP ANY ANY 443

Which of the following solutions would accomplish your task? (Select the two best answers.)

- A. Apply the current ACL to all interfaces of the firewall.
- B. Add the following ACL to the bottom of the current ACL:
Deny IP ANY ANY 53
- C. Add the following ACL to the bottom of the current ACL:
Deny ICMP ANY ANY 53
- D. Remove the current ACL.
- E. Add the following ACL to the top of the current ACL:
Deny TCP ANY ANY 53
- F. Change the default firewall settings so that it implements an implicit deny.

Real-World Scenario 8-1 Solution

The best answers are B and F. Add the following ACL to the bottom of the current ACL: Deny IP ANY ANY 53. Change the firewall default settings so that it implements an implicit deny.

Also, the implicit allow should be removed from the firewall. Most firewalls are configured in the manner of an implicit deny by default. Watch your syntax as well. For example, if you were using a Cisco device, a TCP or UDP deny might require "eg" before the port number. Also, the placement of the ACLs is important.

Video Solution: Watch the video solution "8-1: Access Control Lists."