CCIE Security Version 5
Advanced Technologies Class

Dynamic Access-Lists

What are dynamic ACL's?

Are there any special considerations?

Dynamic Access-Lists Overview

- Are also known as Lock-and-Key ACL
  - Used to authenticate users before allowing network access
  - ACL entries are valid/invalid based on user's authentication status
- Applications
  - Internal user must authenticate before browsing the Internet
  - External user must authenticate before reaching an Internal server

Dynamic Access-Lists Overview

- Considerations
  - Supported only by IPv4 extended ACL
  - ACL must be locally configured on the router
  - A single dynamic ACL entry per ACL is supported
  - User must authenticate via telnet session to the router
- Lock-and-Key ACL was replaced by authentication-proxy
  - Supports more features
  - ACL can be downloaded from the AAA server

Dynamic Access-Lists

Implementation Steps

- Configure the access-list and specify which ACE's are dynamic
- Apply the access-list
- Configure telnet with username based authentication for VTY lines
- Verify its functionality

Dynamic Access-Lists Per-User

- By default once a user authenticates to the router
  - Dynamic ACL entries become valid for all users/source IP's
- Optionally, you can force each user to be authenticated
  - Dynamic ACL entries become valid per user/source IP
- This feature can be configured
  - At the username level
  - At the VTY lines level

Dynamic Access-Lists Timeout

- By default a dynamic ACL entry never times out
  - Potential security risk
- Optionally, two timers are configurable
  - Idle timeout, at the user/VTY level
  - Absolute timeout, at the ACL level