



# Chapter 9

## Cisco IOS Firewall



# IOS Firewall

- ◆ Stateful packet-filter firewall that runs on a router
- ◆ Provides firewall capabilities and normal routing functionality
- ◆ Based on Context-Based Access Control (CBAC)



# Context-Based Access Control

- ◆ Has similar objectives as ASA
- ◆ Dynamically modifies the extended ACLs to allow return traffic of connections established from the inside network
- ◆ Inspects transport level and application level protocols
- ◆ Keeps track of the number and duration of sessions by inspecting packets



# CBAC Protection against Denial of Service Attacks

- ◆ Limits total number of half-open TCP or UDP sessions
- ◆ Limits number of half-open sessions based on time
- ◆ Limits number of half-open sessions per host