CCIE Security Version 5
Advanced Technologies Class

Zone Based Policy Firewall Overview

What is Zone Based Policy Firewall?

What are the functional modes and features?

ZBPF Overview

- What is Zone Based Policy Firewall?
  - Stateful IP firewall implementation on IOS routers
  - Also known as ZBFW, ZFW, ZBPF, ZPF
- Which traffic can be inspected?
  - IPv4 and IPv6 unicast
  - Transit traffic (data-plane)
  - Router generated/destined traffic (control-plane), with some restrictions

ZBPF Overview

- ZBPF is the successor of CBAC, with advanced features
  - Stateful inspection engine (OSI layer 3/4)
  - Application Inspection and Control (OSI layer 7)
  - Built-in DDoS (TCP intercept in watch mode)
  - High Availability with Asymmetric Routing Support
  - NAT integration
  - VRF-aware (supported on both CE and PE)

ZBPF vs. CBAC

- ZBPF allows for more granular control as opposed to CBAC
  - Interfaces are grouped together into zones
  - Firewall policies are unidirectional and based on zone associations
- ZBPF configuration is more modular as compared to CBAC
  - Simplifies design with 3 or more interfaces on the router

ZBPF vs. CBAC

- ZBPF works in closed mode by default
  - All inter-zone traffic is dropped

ZBPF Functional Modes

- ZBPF can be implemented in two modes
  - Routed mode
  - Transparent mode (router behaves like a bridge/switch)