CCIE Security Version 5
Advanced Technologies Class

Zone Based Policy Firewall Building Blocks

What is the command syntax?

What are the building blocks of ZBFW?

What is the default firewall policy?

ZBPF Command Syntax

- ZBPF supports both IPv4 and IPv6

  Via unified and structured command syntax called C3PL

  - http://www.cisco.com/c/en/us/td/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/C3PL.html

ZBPF Building Blocks

- The following blocks are used by ZBPF
  - Zones
  - Class-maps of type inspect
  - Policy-maps of type inspect
  - Zone-pairs
  - PAM (port-to-application mapping)
  - Parameter-maps

ZBPF Zones

- There are two types of zones
  - System defined zones
  - User defined zones

ZBPF System Defined Zones

- System defined zones exist by default
  - Zone **self** (used to define policies for control-plane traffic)
  - Zone **default** (interfaces without zone membership are automatically attached to this zone)
- System defined zones restriction
  - Interface cannot be associated with it

ZBPF User Defines Zones

- User defined zones must be configured manually
  - A zone is defined by giving it an meaningful name
  - Used to define policies for data-plane traffic
- User defined zones restriction
  - Interfaces MUST be associated with it
  - An interface cannot belong to more than one zone

ZBPF Class-Maps

- There are two types of inspect class-maps
  - Layer 3/4 class-maps
  - Layer 7 class-maps

ZBPF Layer 3/4 Class-Maps

- Layer 3/4 inspect class-maps are also named top-level class-maps
  - Used to classify traffic for firewall policies
- Traffic can be classified by matching on
  - Layer 3/4 attributes (access-lists)
  - Layer 4 attributes (makes use of PAM for port numbers)
  - Both of the above
- Layer 3/4 inspect class-maps support nesting
  - For configuration scalability

ZBPF Layer 7 Class-Maps

- Layer 7 inspect class-maps are also named application class-maps
  - Used to match on traffic based on layer 7 criteria
  - Used only for application inspection, not for firewall policies
- Traffic can be classified by matching on
  - Application specific parameters from the layer 7 headers
- Application class-maps cannot be nested
  - Why would you even need that?

ZBPF Layer 3/4 Policy-Maps

- Layer 3/4 inspect policy-maps are also named top-level policy-maps
  - Used to define firewall policies/actions
- There are two types of actions
  - Mandatory/primary (inspect, pass, drop)
  - Optional/secondary (police, log, service-policy)
- Optional actions can only be added to an mandatory action

ZBPF Layer 3/4 Policy-Maps

- Layer 3/4 inspect policy-map mandatory actions
  - Inspect (perform stateful inspection to allow return traffic)
  - Pass (allow traffic without inspection, similar to an ACL permit action)
  - Drop (deny traffic, similar to ACL deny action)
- Pass action should be used for traffic which cannot be inspected, for example
  - ESP and GRE

ZBPF Layer 3/4 Policy-Maps

- Layer 3/4 inspect policy-map optional actions
  - Log (generate a syslog message)
    - Can only be attached to an drop/pass action
  - Police (rate-limit traffic)
    - Can only be attached to an inspect/pass action
  - Service-policy (layer 7 inspection)
    - Can only be attached to an inspect action

ZBPF Layer 7 Policy-Maps

- Layer 7 inspect policy-maps are also named application policy-maps
  - Used to control inspected traffic based on layer 7 header
- Based on the protocol, different actions can be taken
  - Allow
  - Reset
  - Log

ZBPF Zone-Pairs

- Zone-pairs are used to define unidirectional firewall policies
  - Two zones are grouped together (source and destination)
  - A layer 3/4 policy-map is attached to it

ZBPF PAM

- Port-to-application mapping (PAM)
  - Used to classify traffic based on well-known TCP/UDP port numbers used by services (like FTP, HTTP)
- Two types of PAM entries exist
  - System defined
  - User defined

ZBPF PAM

- System defined PAM entries
  - Matches on the pre-defined TCP/UDP port numbers of common services
- User defined PAM entries
  - Matches on user-defined TCP/UDP port numbers of common services
  - Used whenever an application does not use the default TCP/UDP port numbers
- Per IP address user-defined entries are supported

ZBPF Parameter-Maps

- Parameter-maps are used for advanced ZBFW features
  - Enable High Availability
  - TCP Out-Of-Order packet handling
  - Configure DDoS settings
  - Configure local URL filtering or integration with CWS
  - Define REGEX used in application inspection
- Several parameter-map types exist, based on the scope
  - Main used one is of the type **inspect**

ZBPF Firewall Policies

- Once interfaces have been assigned to zones, without any firewall policy defined
  - All control-plane traffic works in a **pass** mode in both directions
  - All inter-zone data-plane traffic works in **drop** mode in both directions
  - All intra-zone data-plane traffic works in a **pass** mode in both directions
- These can be changed via firewall policies

ZBPF Firewall Policies

- Traffic between an interface associated with a zone and one without associated to a zone
  - Is dropped and cannot be fixed