CCIE Security Version 5 Advanced Technologies Class

Access-Lists Overview

What are access-lists and their scope?

What are the access-list types?

Access-Lists Overview

- What are access-lists?
  - Used for traffic classification
  - Matches on the layer2/layer3/layer4 header
- ACL Types
  - Non-IP (matches on the layer 2 header)
  - IP (matches on the layer3/layer4 header)
- IP ACL Types
  - IPv4
  - IPv6

IP Access-Lists Overview

▷What is the scope of IP access-lists?

- Control Plane: Route Filtering and Administrative Distance
- Management Plane: VTY, SNMP, NTP Security
- Data Plane: Packet Filtering
- Services Plane: NAT, IPsec, QoS, policy routing

IPv4 Access-List Types

- Can be of two types
  - Standard
  - Extended
- Configuration wise, both standard and extended can be
  - Numbered (legacy, identified by a number)
  - Named (identified by a meaningful name)

IPv6 Access-List Types

- With IPv6 ACL, legacy features are not supported
  - Only extended named ACL's are supported

Access-Lists Packet Filtering

▷When used for Packet Filtering

- ACL must be applied at the interface level, in or out
- There can be a single ACL applied per interface, per direction, per protocol

▷Matched Traffic Per Direction

- Inbound ACL matches on both control and data plane traffic
- Outbound ACL matches only on data plane traffic

Standard Access-Lists

▷Standard ACL

- Matches only on the source IP from the IP header

▷Standard ACL Restrictions

- Cannot match on the layer3 protocol (it has to be IPv4)
- Cannot match on the layer4 header

▷Standard ACL Exceptions

- Matches on the destination IP from the IP header if used for VTY lines restriction in the outbound direction

Extended Access-Lists

▷Extended ACL

- Can match the protocol number from the layer 3 header (OSPF, EIGRP, ESP, AH)
- Can match on both source and destination IP from the layer 3 header
- Can match on the layer 4 protocol and its ports (TCP, UDP)

Extended Access-Lists

- Extended ACL
  - Can match on the TCP flags, IPv4/IPv6 options
  - Can match on IPv4/IPv6 fragments
  - Can match on IPv4/IPv6 packet marking (Precedence, DSCP)

Knowledge is Power!