CCIE Security Version 5
Advanced Technologies Class

Reflexive Access-Lists

What are reflexive ACL's?

Are there any special considerations?

Access-Lists Overview

- By default, when used for traffic filtering
  - ACL's are stateless packet filters
- ACL's can be configured to be session-aware, but not like a full-blown stateful firewall
  - Allows for more secure and scalable packet filtering
- Session-aware ACL's
  - Via the 'established' keyword when ACL entry is defined
  - Via reflexive ACL's

Access-Lists with 'Established'

- If 'established' keyword is specified to an ACL entry
  - It only works for TCP statements
  - ACL entry is matched if the **RST** and/or **ACK** flags are set
- Applications
  - Dropping any legit TCP session initiated in the reverse direction
- Legit TCP session
  - The first packet only has the **SYN** flag set

Reflexive Access-Lists Overview

- The first attempt to create a stateful firewall
  - Router inspects packets matched by an ACL and flowing in one direction
  - Router automatically opens dynamic holes in the reverse direction ACL to allow for return traffic (reflection)
- What does the router inspect
  - TCP, UDP, ICMP
  - For TCP/UDP it keeps track of layer3/layer4 information
  - For ICMP it keeps track of layer 3 information and only works for Echo-Request/Echo-Reply

Reflexive Access-Lists Overview

Considerations

- Supported for IPv4/IPv6 traffic via extended ACL's
- Deep Packet Inspection (DPI) is not supported
- Protocols that open secondary sessions (FTP, TFTP) are not supported if secondary session is opened in reverse direction of the inspection

Reflexive Access-Lists

Implementation Steps

- Configure the reflexive ACL defining which traffic is inspected and apply it in the outbound direction
- Configure the ACL defining which traffic is allowed in the reverse direction and reference the reflexive ACL
- Verify its functionality

Reflexive Access-Lists Timeout

- By default the dynamically opened hole in the return ACL
  - Expires after 5 minutes of inactivity