ENCOR v1.1 (350-401) Video Training Series
Module 5 – Lesson 2 Quiz

Questions

1. Which of the following is considered to be a standard numbered access control list (ACL)?

   A. 100
   B. 1300
   C. 199
   D. 2000

2. Which type of access control list (ACL) allows us to match traffic source and destination IP addresses?

   A. Expanded ACLs
   B. IP ACLs
   C. Standard ACLs
   D. Extended ACLs

3. Which type of access control list (ACL) should be placed as close to the source as possible?

   A. Standard ACL
   B. Extended ACL
   C. Source ACL
   D. Destination ACL

4. Which entity within the Control Plane Policing (CoPP) solution allows for traffic filtering and rate limiting?

   A. ACL
   B. QoS
   C. MQC
   D. SNMP

Questions and Answers

1. Which of the following is considered to be a standard numbered access control list (ACL)?

   A. 100
   B. 1300
   C. 199
   D. 2000

Answer: B
Explanation: Standard numbered access control lists (ACLs) fall within the range of 1-99. There is also an extended range in case you need additional standard numbered ACLs, which fall within the range of 1300-1999.

Video Reference: Standard Access Control List (ACL) Configuration

2. Which type of access control list (ACL) allows us to match traffic source and destination IP addresses?

   A. Expanded ACLs
   B. IP ACLs
   C. Standard ACLs
   D. Extended ACLs

Answer: D
Explanation: Extended access control lists (ACLs) fall within the range of 100-199, with an expanded range of 2000-2699. These have the ability to filter much more granularly than standard ACLs, as they are able to filter specific protocols and match both source and destination IP addresses.

Video Reference: Extended Numbered ACL Configuration

3. Which type of access control list (ACL) should be placed as close to the source as possible?

   A. Standard ACL
   B. Extended ACL
   C. Source ACL
   D. Destination ACL

Answer: B
Explanation: Extended ACLs have the ability to filter between protocol types and can match traffic based on both source and destination IP addressing. Because of the ability to see IP addressing in this way, a best practice recommendation is to place extended ACLs as close to the source as possible in order to stop traffic early on. This ensures that unwanted traffic doesn't take up network bandwidth unnecessarily. The opposite is true of standard ACLs, which are recommended to be placed as close to the destination as possible.

Video Reference: ACL Considerations

4. Which entity within the Control Plane Policing (CoPP) solution allows for traffic filtering and rate limiting?

   A. ACL
   B. QoS
   C. MQC
   D. SNMP

Answer: C
Explanation: Modular QoS CLI (MQC) allows for both filtering and rate-limiting of our network traffic. Within MQC, we have the ability to create and attach a traffic policy to an interface. ACLs are used to identify the traffic itself, against which we want to take action with MQC. Filtering and rate limiting are not performed by the ACL itself, but rather it is only used for traffic identification. The MQC policy is what allows for the filtering and rate-limiting.

Video Reference: Control Plane Policing (CoPP) Theory