Exam Code: HP0-757

Exam Name: HP ProCurve Security

Vendor: HP

Version: DEMO

Part: A

1: What is true with regard to standard and extended access control lists (ACLs) on the HP ProCurve 5300xl?
A.A standard ACL can only specify a filter based on a destination IP address, while an extended ACL can specify both source and destination IP addresses.
B.Standard and extended ACLs can both specify Layer 4 TCP/UDP ports, but only an extended ACL can specify precedence and type of service traffic.
C.An extended ACL can filter traffic from a source TCP/UDP port to a destination IP address, while a standard ACL only supports filters based on the source IP address.
D.An extended ACL supports filtering on both source and destination TCP/UDP ports, while a standard ACL only supports source TCP/UDP ports.
Correct Answers: C

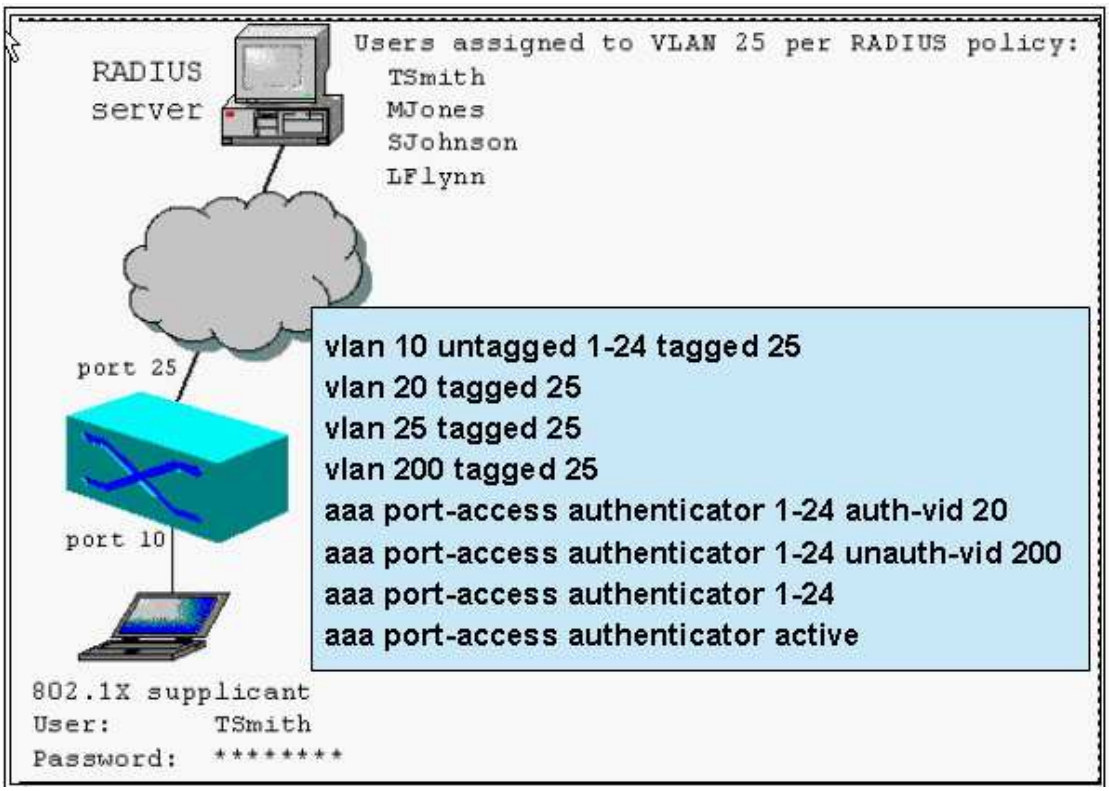
2: You have enabled port security using the "send-disable" action. Which administrative action, if any, is required after an intrusion to enable the device to return to normal operation?
A.No action is required.
B.The intrusion flag must be cleared.
C.The port must be enabled.
D.The intrusion flag must be cleared and the port must be enabled.
Correct Answers: D

3: You support a network that has ports in a conference room that is regularly used by guests. You have decided to define a guest VLAN that allows access to the internet and prevents access to corporate resources. Which solution provides the most flexibility and lowest management overhead while placing the guest users in the appropriate VLAN?
A.Require that guests connect only to ports in the conference room that are members of the guest VLAN.
B.Enable 802.1X on the conference room ports. Give guests a temporary logon ID and provide them with 802.1X supplicant software. Associate guest user IDs with a guest VLAN that prevents access to corporate resources.
C.Enable IEEE 802.1X on the conference room ports and configure the guest VLAN as the authorized VLAN for these ports.
D.Enable IEEE 802.1X on the conference room ports and configure the guest VLAN as the unauthorized VLAN for these ports.
Correct Answers: D

4: In an 802.1X authentication environment there are different methods by which a user can be placed on a VLAN. Which method has the highest priority on a given port?
A.an authorized VLAN assignment configured on the switch at the time 802.1X was enabled for the port
B.a dynamic VLAN assignment from the RADIUS server
C.the statically assigned VLAN configured for the port
D.the priority determined by the command used to configure the port for 802.1X authentication

Correct Answers: B

5: Click the Exhibit button.
The RADIUS server and switch are correctly configured for proper interaction. The switch has the VLAN assignments and port-access commands shown in the diagram. When the user provides valid authentication information, port 10 will _____.



A.remain in an unauthorized state and prevent user traffic from being forwarded
B.become a member of VLAN 20
C.become a member of VLAN 25
D.become a member of VLAN 200
Correct Answers: C

6: Which statement is true with regard to the AAA security framework? It _____.
A.defines standardized processes for access, authorization, and accountability
B.defines standardized processes for authentication, authorization, and accounting
C.is an application-neutral Internet standard that defines access control for layer 3 switches
D.is an HP-proprietary specification that defines how HP ProCurve switches process login sessions
Correct Answers: B

7: A network administrator wants to prevent users in the marketing department from accessing servers on the finance network. Both departments are connected to the network with an 5300xl switch. Finance department users should have access to the finance servers as well as other common network resources. Which measures combined would accomplish this goal? Select TWO.

A.Enforce resource operating system security on the finance servers in the form of user names and passwords.
B.Place marketing department users in a different VLAN than the finance servers.
C.Apply access control lists to router interfaces to prevent unauthorized traffic from reaching the finance servers.
D.Isolate the "problem" users in the marketing department by placing them in a separate physical network.
E.Provide multiple physical interfaces for the finance server.
Correct Answers: B C

8: What is the main difference between EAP-TLS and EAP-MD5?
A.EAP-TLS uses a challenge/handshake mechanism for authentication; EAP-MD5 uses certificates for authentication.
B.EAP-TLS uses a challenge/handshake mechanism for authentication and encryption; EAP-MD5 uses certificates for authentication and encryption.
C.EAP-TLS uses a name and password along with digital certificates to produce a session key; EAP-MD5 uses a name and password to produce a session key.
D.EAP-TLS uses digital certificates for mutual authentication; EAP-MD5 uses a challenge/handshake mechanism to authenticate the client to the server.
Correct Answers: D

9: A customer wants to provide stricter access security for all network clients and implement a combination of 802.1X and MAC authentication. Which parameters must be configured on the RADIUS server to support the ports configured with MAC authentication? Select TWO.
A.Configure PAP to support unencrypted authentication of network peripherals.
B.Create a user on the RADIUS server using the MAC address of the device for the username and the password.
C.Create a user on the RADIUS server using the MAC address of the device for the username and the RADIUS shared secret for the password.
D.Configure CHAP RADIUS for the authentication method.
E.Create a user on the RADIUS server using the MAC address of the device for the username and do not configure a password (leave it blank).
F.Configure EAP RADIUS for the authentication method.
Correct Answers: B D

10: The network administrator of a private college wants to enable web authentication for all access ports in the student housing buildings. In addition, he wants to address the growing problem of students using unauthorized switches to network more than one device per access port. What additional configuration is required to prevent more than one authenticated user from connecting to a port that has default web authentication enabled?
A.Enable port security with the address-limit 1 option.
B.The default client limit is 1 for Web authentication so no further configuration is required.
C.Enable port security with the learn-mode port-access option.
D.Add an option to the port-access command that limits the number of MAC addresses to 1.

Correct Answers: B