VirtuLearn

TRUSTED, ACCURATE AND RELIABLE!

The most comprehensive IT certification preparation materials in the industry!

https://www.virtulearner.com
support@virtulearner.com

HP

HPE6-A84

Aruba Certified Network Security Expert Written Certification Exam

QUESTION: 1
You are designing an Aruba ClearPass Policy Manager (CPPM) solution for a customer. You learn that the customer has a Palo Alto firewall that filters traffic between clients in the campus and the data center.

Which integration can you suggest?

A. Sending Syslogs from the firewall to CPPM to signal CPPM to change the authentication status for misbehaving clients
B. Importing clients' MAC addresses to configure known clients for MAC authentication more quickly
C. Establishing a double layer of authentication at both the campus edge and the data center DMZ
D. Importing the firewall's rules to program downloadable user roles for AOS-CX switches more quickly

Answer(s): A

Explanation:
This option allows CPPM to receive real-time information about the network activity and security posture of the clients from the firewall, and then apply appropriate enforcement actions based on the configured policies. For example, if a client is detected to be infected with malware or violating the network usage policy, CPPM can quarantine or disconnect the client from the network.

QUESTION: 2
Refer to the scenario.

A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

Switches are using local port-access policies.

The customer wants to start tunneling wired clients that pass user authentication only to an Aruba gateway cluster. The gateway cluster should assign these clients to the "eth-internet" role. The gateway should also handle assigning clients to their VLAN, which is VLAN 20.

The plan for the enforcement policy and profiles is shown below:

The gateway cluster has two gateways with these IP addresses:

· Gateway 1
o VLAN 4085 (system IP) = 10.20.4.21
o VLAN 20 (users) = 10.20.20.1
o VLAN 4094 (WAN) = 198.51.100.14
· Gateway 2
o VLAN 4085 (system IP) = 10.20.4.22
o VLAN 20 (users) = 10.20.20.2
o VLAN 4094 (WAN) = 198.51.100.12
· VRRP on VLAN 20 = 10.20.20.254

The customer requires high availability for the tunnels between the switches and the gateway cluster. If one gateway falls, the other gateway should take over its tunnels. Also, the switch should be able to discover the gateway cluster regardless of whether one of the gateways is in the cluster.

You are setting up the UBT zone on an AOS-CX switch.

Which IP addresses should you define in the zone?

A. Primary controller = 10.20.4.21; backup controller = 10.20.4.22
B. [Primary controller = 198.51.100.14; backup controller = 10.20.4.21
C. Primary controller = 10 20 4 21: backup controller not defined
D. Primary controller = 10.20.20.254; backup controller, not defined

Answer(s): A

Explanation:
To configure user-based tunneling (UBT) on an AOS-CX switch, you need to specify the IP addresses of the mobility gateways that will receive the tunneled traffic from the switch. The primary controller is the preferred gateway for the switch to establish a tunnel, and the backup controller is the alternative gateway in case the primary controller fails or becomes unreachable. The IP addresses of the gateways should be their system IP addresses, which are used for inter-controller communication and cluster discovery.
In this scenario, the customer has a gateway cluster with two gateways, each with a system IP address on VLAN 4085. Therefore, the switch should use these system IP addresses as the primary and backup controllers for UBT. The IP addresses of the gateways on VLAN 20 and VLAN 4094 are not relevant for UBT, as they are used for user traffic and WAN connectivity, respectively. The VRRP IP address on VLAN 20 is also not applicable for UBT, as it is a virtual IP address that is not associated with any specific gateway.
Therefore, the best option is to use 10.20.4.21 as the primary controller and 10.20.4.22 as the backup controller for UBT on the switch. This will ensure high availability and cluster discovery for the tunneled traffic from the switch to the gateway cluster.

QUESTION: 3
Refer to the scenario.

A customer requires these rights for clients in the "medical-mobile" AOS firewall role on Aruba Mobility Controllers (MCs):

Permitted to receive IP addresses with DHCP
Permitted access to DNS services from 10.8.9.7 and no other server
Permitted access to all subnets in the 10.1.0.0/16 range except denied access to 10.1.12.0/22
Denied access to other 10.0.0.0/8 subnets
Permitted access to the Internet
Denied access to the WLAN for a period of time if they send any SSH traffic
Denied access to the WLAN for a period of time if they send any Telnet traffic
Denied access to all high-risk websites
External devices should not be permitted to initiate sessions with "medical-mobile" clients, only send return traffic.

The exhibits below show the configuration for the role.