HPE6-A84 Q&As

Aruba Certified Network Security Expert Written

Pass HP HPE6-A84 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/hpe6-a84.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

Refer to the scenario.

A customer has asked you to review their AOS-CX switches for potential vulnerabilities. The configuration for these switches is shown below:

```
hostname Access-Switch-$$

ntp authentication-key 1 sha1 ciphertext
AQBapYn45h7mDzxcLhAYWBH6biegegFASS1kvTQPPgICEfaLCAAAAMIb48QNRhSg
ntp trusted-key 1
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst key-id 1
ntp enable
ntp authentication
!
radius-server host rad.example.com tls
!
tacacs-server host rad.example.com
!
aaa authentication login ssh group tacacs local
aaa authentication login telnet group tacacs local
!
aaa accounting port-access start-stop interim group radius
!
radius dyn-authorization enable
!
radius dyn-authorization client rad.example.com tls
ssh server vrf default
ssh server vrf mgmt
telnet server vrf default
telnet server vrf mgmt
crypto pki application radsec-client certificate device-identity
crypto pki ta-profile privateca
ta-certificate
      -----BEGIN CERTIFICATE-----
      MIIGAzCCA+ugAwIBAgIUEVfsxopuixT2QHZDJ/UYAAbYsdowDQYJKoZIhvcNAQEL
      BQAwgYgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQH
      DAlTdW5ueXZhbGUxHDAaBgNVBAoME0FydWJhIFRyYWluaW5nIExhYnMxEzARBgNV
      BAsMCkFDTlNYIFRlc3QxHTAbBgNVBAMMFHJvb3RjYS5hY25zeHRlc3QuY29tMB4X
      DTIyMTEyMjIwNTQxOFoXDTMyMTExOTIwNTQxOFowgYgxCzAJBgNVBAYTAlVTMRMw
      EQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQHDAlTdW5ueXZhbGUxHDAaBgNVBAoM
      E0FydWJhIFRyYWluaW5nIExhYnMxEzARBgNVBAsMCkFDTlNYIFRlc3QxHTAbBgNV
      BAMMFHJvb3RjYS5hY25zeHRlc3QuY29tMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
      MIICCgKCAgEAsiUzsBkJcUgcdsbRyoLd0ZNqpcXfphk2VsSzZngP1LCu3lea3OHU
      V9GchhJXOQaI3HDUTcLp4b5If63z4nKzA36T6tyWXOe0PSgUjy+61XXMA9Rp5DKc
      CyoY9F8spVJiEo2n2hqL4m/DLFYlhxo5Z2UKav/08DMfzD/yVUzGNiQKDP/L7ivk
      CWF+15WIGSrH10i/rgIM/+W20n58aDx5f1AWaH9DYdRTWFMuk1UXQ/I8+7+9PXju
      B95Mt4b77RaWWj6CkW9k8WhmyjE7MMPSHtuJ4t3evh7jd/lTkm5ZOg/V8kvNTtW5
      fif7lkWLevmlLlvcxYnj+S3CWhAFdaR7S33a6xwdZxCDOLfPB6L1oOnKe0VM4mO2
      lOZtJNPFueBt16BRolR+IMANQkj3B2lB0whSLHF6JmLr0L6y/edV8XhIUhMxOfIp
      JKeSw38TDm3t1k98PBCOaLj5s4tYJRxcZLDnrg7Oz1e37sxENYoBtgRp77cdfePr
      cP/sp8U66gti2F0ijkU6k37moL3sMs2uHgC0YWpfRyFI09BWCRbxmy81UePiSlsW
      0goOaPDr35W/0443I/z6A+q/ciwVrALS+zEfHbMDFxo4VMygJttaiWZ05GAQQSHj
      redQmQEQPMwkgbzaELtAgYOWGkB56T/XifRLVxneYU8woAEZwmscI3kCAwEAAaNj
      MGEwHQYDVR0OBBYEFGXCH/z475pdNKIHhjDxFCfjz8khMB8GA1UdIwQYMBaAFGXC
      H/z475pdNKIHhjDxFCfjz8khMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
      AgGGMA0GCSqGSIb3DQEBCwUAA4ICAQB5TGIspaamHQXtsnWgmux6PANdEdPZ0Ele
      wDnpUxkVbeSPr9wl8luRJMptRO25rwVwEtrM8t5JD4jAK+d0usr4TDKwWqPPqFi0
      F5svFK9aEJ59ceD+eDWl4LAJJi3zjb9ZBuBa3LkaP7kyTlSnI0+opN+vdV43LNXh
      T23xEmLC9OUolq3bb8zpkWXieeFwSo2BafFMscPdf75DVY+x+Qo1SgpjbWBAS80B
      jRdZHrKmsqcrIG+37bixqaFj9nMzWpX0n2HfKCVcl6uk2pDNbiYVbU3k9b/ZWQmW
      DRYkAuR8dFBN3lKDyQo86T/chT/DY77FoStfg0gDZEj3EqaM76rf8S2z1GCsrfkp
      Crp5oKP6jiOCi2EcidkZSsmbzAHWKXNaF7vWRj0OivpqEFRkIVu/kce9O2KaxNYd
      sIKlNh7gG4pcQqhFfDddFD9vXvjOwKnXKkKppUpN6w+Quc+jhqFpP8GVPOy7ayZo
      z5cz5yEaVXtbfXRhVSg9oooq7xImBT14SK1pyrHSj8sD67Og3zgnNot/v8fHhI3O
      zUtBe4UPGWfraO4gkHH3mbb1qYeJnxKpMz56A0APBkKV9icY0uTQOsHk6bA9lG+Q
      sjqyWwKApf7RB4lHjF+7FfMU6UJnZBm75zQ89CPAPCoVeJ6fNNr/aO+3VrNz4j9l
      Nr63M6xeYw==
      -----END CERTIFICATE-----
        END_OF_CERTIFICATE
vsf member 1
    type jl666a
dhcpv4-snooping
vlan 1
vlan 2
vlan 4
    dhcpv4-snooping
spanning-tree
interface mgmt
    no shutdown
aaa authentication port-access dot1x authenticator
    enable
interface lag 1
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 2,4
    dhcpv4-snooping trust
interface 1/1/1-1/1/24
    no shutdown
    no routing
    vlan access 4
    aaa authentication port-access dot1x authenticator
        enable
interface vlan 1
interface vlan 2
    ip address 10.1.2.1/24
ip route 0.0.0.0/0 10.1.2.254
ip dns domain-name example.com
ip dns server-address 10.1.1.9
!
https-server vrf default
https-server vrf mgmt
```

What is one recommendation to make?

A. Let the RADIUS server confiqure VLANs on LAG 1 dynamically.

B. Use MDS instead of SHA1 for the NTP authentication key.

C. Encrypt the certificate in the TA-profile.

D. Create a control plane ACL to limit the sources that can access the switch with SSH.

Correct Answer: D

According to the AOS-CX Switches Multiple Vulnerabilities1, one of the vulnerabilities (CVE-2021-41000) affects the SSH service on AOS-CX switches. This vulnerability allows an unauthenticated remote attacker to cause a denial-of-service condition on the switch by sending specially crafted SSH packets. The impact of this vulnerability is high, as it could result in a loss of management access and network disruption. Therefore, one recommendation to make is to create a control plane ACL to limit the sources that can access the switch with SSH. This way, the switch can filter out unwanted or malicious SSH traffic and reduce the risk of exploitation.

QUESTION 2

You are configuring gateway IDS/IPS settings in Aruba Central.

For which reason would you set the Fail Strategy to Bypass?

A. To permit traffic if the IPS engine falls to inspect It

B. To enable the gateway to honor the allowlist settings configured in IDS/IPS policies

C. To tell gateways to stop enforcing IDS/IPS policies if they lose connectivity to the Internet

D. To avoid wasting IPS engine resources on filtering traffic for unauthenticated clients

Correct Answer: A

The Fail Strategy is a configuration option for the IPS mode of inspection on Aruba gateways. It defines the action to be taken when the IPS engine crashes and cannot inspect the traffic. There are two possible options for the Fail Strategy: Bypass and Block1 If you set the Fail Strategy to Bypass, you are telling the gateway to allow the traffic to flow without inspection when the IPS engine fails. This option ensures that there is no disruption in the network connectivity, but it also exposes the network to potential threats that are not detected or prevented by the IPS engine1 If you set the Fail Strategy to Block, you are telling the gateway to stop the traffic flow until the IPS engine resumes inspection. This option ensures that there is no compromise in the network security, but it also causes a loss of network connectivity for the duration of the IPS engine failure1

QUESTION 3

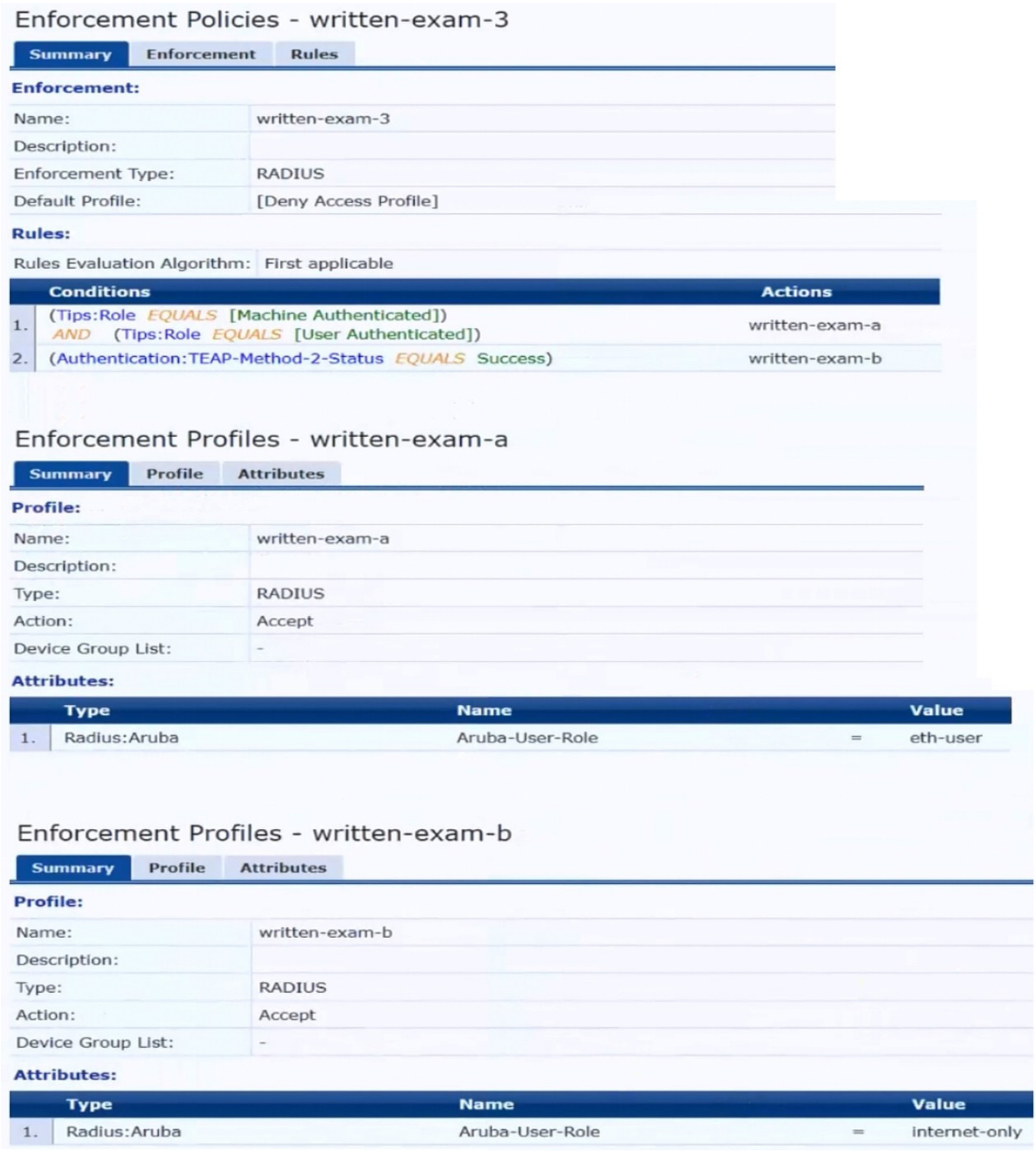
Refer to the scenario.

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

1.

VLAN 4085 (system IP) = 10.20.4.21

2.

VLAN 20 (users) = 10.20.20.1

3.

VLAN 4094 (WAN) = 198.51.100.14

Gateway 2

1.

VLAN 4085 (system IP) = 10.20.4.22

2.

VLAN 20 (users) = 10.20.20.2

3.

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

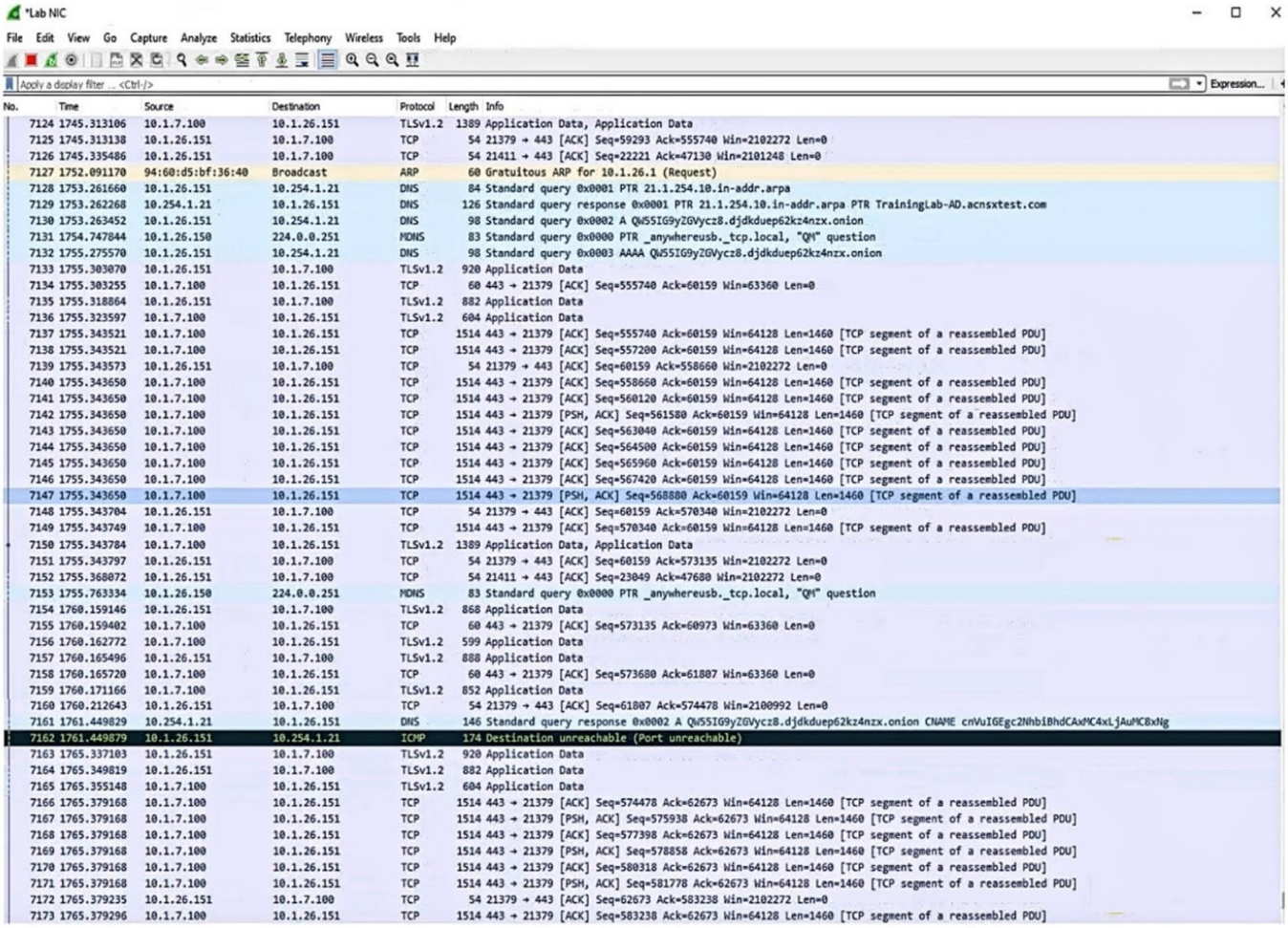
Correct Answer: A

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 1. 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 1. The IP addresses of the gateways should be their system IP addresses, which are used for inter-controller communication and cluster discovery 2. 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 2. 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 3. 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 4

Refer to the exhibit.



Which security issue is possibly indicated by this traffic capture?

A. An attempt at a DoS attack by a device acting as an unauthorized DNS server

B. A port scan being run on the 10.1.7.0/24 subnet

C. A command and control channel established with DNS tunneling

D. An ARP poisoning or man-in-the-middle attempt by the device at 94:60:d5:bf:36:40

Correct Answer: C

DNS tunneling is a technique that abuses the DNS protocol to tunnel data or commands between a compromised host and an attacker\\'s server. DNS tunneling can be used to establish a command and control channel, which allows the attacker to remotely control the malware or exfiltrate data from the infected host1 The traffic capture in the exhibit shows some signs of DNS tunneling. The source IP address is 10.1.7.2, which is likely an internal host behind a firewall. The destination IP address is 8.8.8.8, which is a public DNS resolver. The DNS queries are for subdomains of badsite.com,

which is likely a malicious domain registered by the attacker. The subdomains have long and random names, such as 0x2a0x2a0x2a0x2a0x2a0x2a0x2a0x2a.badsite.com, which could be used to encode data or commands. The DNS responses have large sizes, such as 512 bytes, which could be used to carry data or commands back to the host2

QUESTION 5

Refer to the scenario.

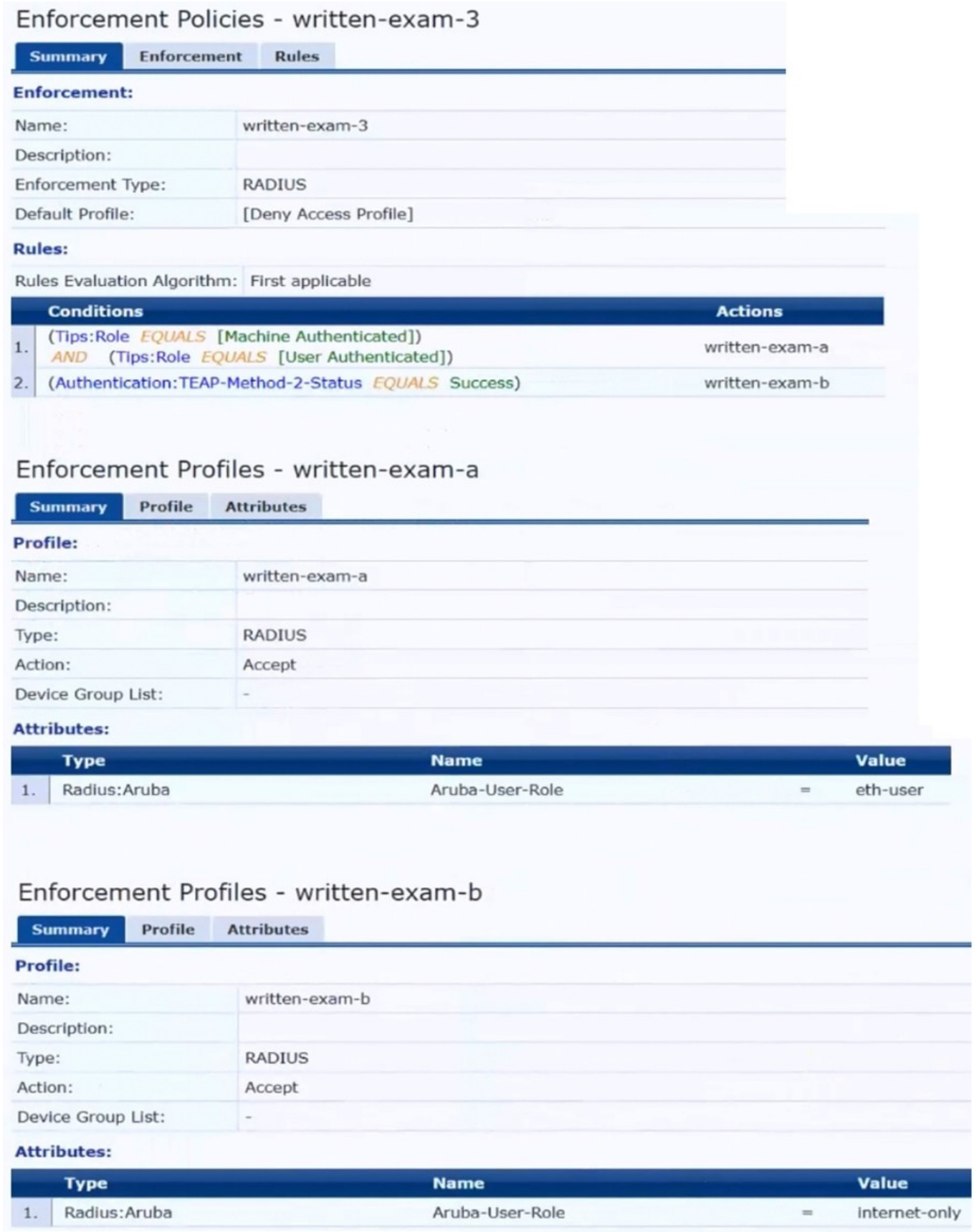
A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

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:



Enforcement Policies - written-exam-3

Summary | Enforcement | Rules

Enforcement:

Name:	written-exam-3
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS [Machine Authenticated]) AND (Tips:Role EQUALS [User Authenticated])	written-exam-a
2.	(Authentication:TEAP-Method-2-Status EQUALS Success)	written-exam-b

Enforcement Profiles - written-exam-a

Summary | Profile | Attributes

Profile:

Name:	written-exam-a
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	eth-user

Enforcement Profiles - written-exam-b

Summary | Profile | Attributes

Profile:

Name:	written-exam-b
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	internet-only

The gateway cluster has two gateways with these IP addresses:

Gateway 1

1.

VLAN 4085 (system IP) = 10.20.4.21

2.

VLAN 20 (users) = 10.20.20.1

3.

VLAN 4094 (WAN) = 198.51.100.14

Gateway 2

1.

VLAN 4085 (system IP) = 10.20.4.22

2.

VLAN 20 (users) = 10.20.20.2

3.

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.

Assume that you are using the "myzone" name for the UBT zone.

Which is a valid minimal configuration for the AOS-CX port-access roles?

A. port-access role eth-internet gateway-zone zone myzone gateway-role eth-user

B. port-access role internet-only gateway-zone zone myzone gateway-role eth-internet

C. port-access role eth-internet gateway-zone zone myzone gateway-role eth-internet vlan access 20

D. port-access role internet-only gateway-zone zone myzone gateway-role eth-internet vlan access 20

Correct Answer: B

The UBT solution requires that the edge ports on the switches are configured in VLAN trunk mode, not access mode. This is because the UBT solution uses a special VLAN (VLAN 4095 by default) to encapsulate the user traffic and tunnel it to the gateway. The edge ports need to allow this VLAN as well as any other VLANs that are used for management or control traffic. Therefore, the edge ports should be configured as VLAN trunk ports and allow the necessary VLANs