HPE6-A78시험문제집즉덤프가지니고있는장점 - Aruba Certified Network Security Associate Exam
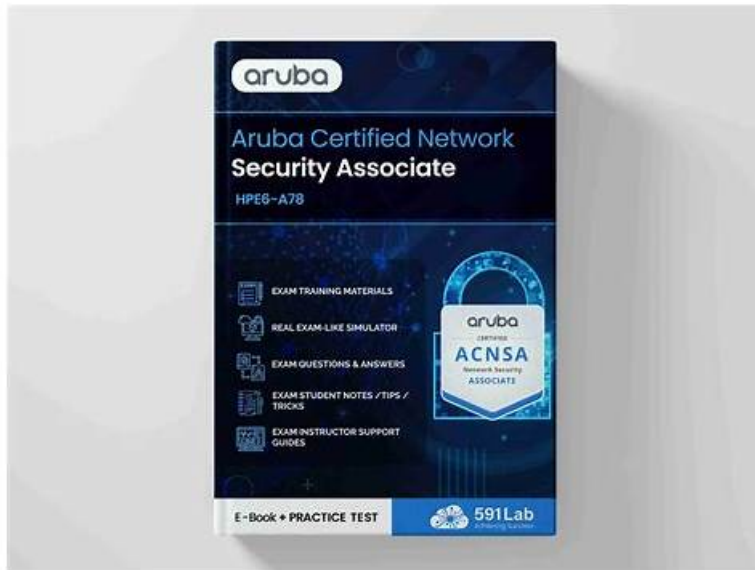
HP HPE6-A78 덤프의 PDF 버전과 Software 버전의 내용은 동일합니다. PDF버전은 프린트 가능한 버전으로서 단독 구매하셔도 됩니다. Software 버전은 테스트용으로 PDF 버전 공부를 마친후 시험전에 실력테스트 가능합니다. Software 버전은 PDF버전의 보조용이기에 단독 판매하지 않습니다. 소프트웨어버전까지 필요하신 분은 PDF버전을 구입하실때 공동구매하셔야 합니다.

HP HPE6-A78 시험은 네트워크 보안 전문가들의 지식과 기술을 시험하는 자격증 시험으로, 네트워크 보안 및 무선 네트워킹에서 기술과 지식을 향상시키고자 하는 사람들을 대상으로 합니다. 이 자격증은 산업에서 광범위하게 인정받는 Aruba Certified Network Security Associate (ACNSA) 자격증에 특별히 초점을 맞추고 있습니다. 이 시험은 다양한 네트워크 보안 주제를 다루며 도전적이므로, 네트워크 보안 전문가들이 네트워크 보안 및 무선 네트워킹에서 기술과 지식을 향상시키기에 이상적입니다.

**>> HPE6-A78높은 통과율 덤프문제 <<**

HPE6-A78인기덤프문제 & HPE6-A78시험대비 덤프 최신 데모

Itcertkr에서 출시한 HP인증 HPE6-A78덤프는HP인증 HPE6-A78시험에 대비하여 IT전문가들이 제작한 최신버전 공부자료로서 시험패스율이 100%입니다.Itcertkr는 고품질 HP인증 HPE6-A78덤프를 가장 친근한 가격으로 미래의 IT전문가들께 제공해드립니다. Itcertkr의 소원대로 멋진 IT전문가도 거듭나세요.

HP HPE6-A78 자격증 시험은 보안 프로토콜, 접근 제어, 방화벽, 침입 탐지 및 예방 시스템과 관련된 다양한 주제를 다룹니다. 이 시험은 또한 보안 정책 및 절차, 위험 평가, 규정 준수 등을 다룹니다. 이 자격증은 네트워크 보안 전문가들이 경력을 발전시키고 네트워크 보안 전문가로서의 전문성을 입증하려는 경우 필수 자격증입니다. 이 자격증 프로그램은 종합적인 교육 프로그램을 제공하여 개인이 시험에 대비하고 Aruba Certified Network Security Associates 자격증을 취득하기 위해 필요한 기술과 지식을 습득할 수 있도록 돕습니다.

HP HPE6-A78 자격증 시험은 Aruba 제품과 솔루션을 다루는 네트워크 보안 전문가들에게 필수적인 자격증입니다. 이는 후보자의 네트워크 보안 지식과 전문성을 입증하며 이 분야에서의 경력 향상을 위한 중요한 기초를 제공합니다.

최신 Aruba ACNSA HPE6-A78 무료샘플문제 (Q121-Q126):

질문 # 121
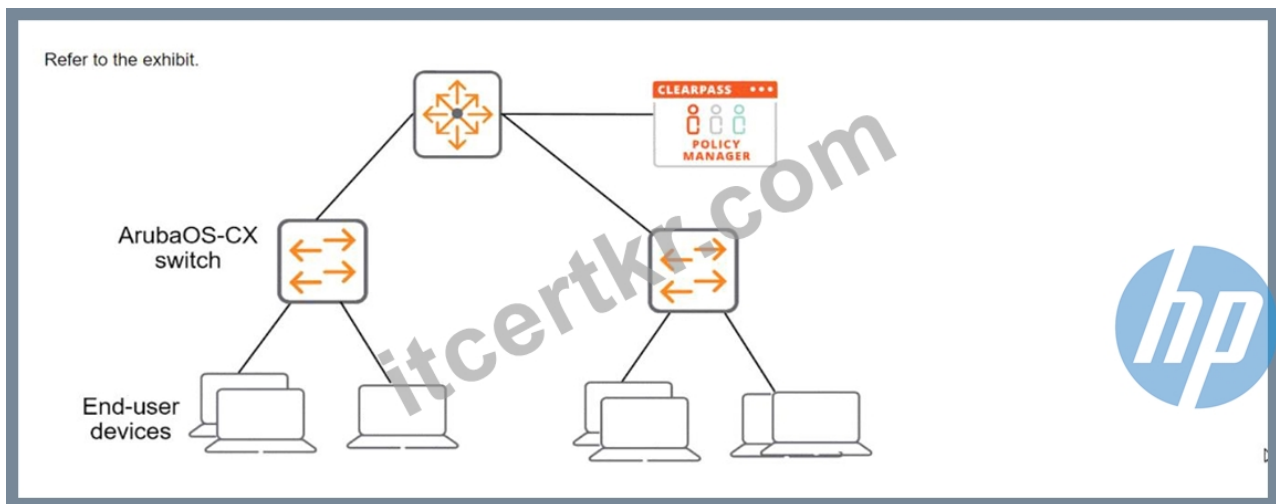
What is another setting that you must configure on the switch to meet these requirements?

- A. Disable SSH on the default VRF and enable it on the mgmt VRF instead.
- B. Configure a CPPM username and password that match a CPPM admin account.
- C. Set the aaa authentication login method for SSH to the "radius" server-group (with local as backup).
- D. Create port-access roles with the same names of the roles that CPPM will send in Aruba-Admin-Role VSAs.

정답：C

설명：

To meet the requirements for configuring an ArubaOS-CX switch for integration with ClearPass Policy Manager (CPPM), it is necessary to set the AAA authentication login method for SSH to use the "radius" server-group, with "local" as a backup. This ensures that when an admin attempts to SSH into the switch, the authentication request is first sent to CPPM via RADIUS. If CPPM is unavailable, the switch will fall back to using local authentication12.

Here's why the other options are not correct:

Option B is incorrect because configuring a CPPM username and password on the switch that matches a CPPM admin account is not required for SSH login; rather, the switch needs to be configured to communicate with CPPM for authentication.

Option C is incorrect because while CPPM will send Aruba-Admin-Role Vendor-Specific Attributes (VSAs), the switch does not need to have port-access roles created with the same names; it needs to interpret the VSA to assign the correct role.

Option D is incorrect because disabling SSH on the default VRF and enabling it on the mgmt VRF is not related to the authentication process with CPPM.

Therefore, the correct answer is A, as setting the AAA authentication login method for SSH to the "radius" server-group with "local" as backup is a key step in ensuring that the switch can authenticate admins through CPPM while providing a fallback method12.

질문 # 122

Refer to the exhibit.
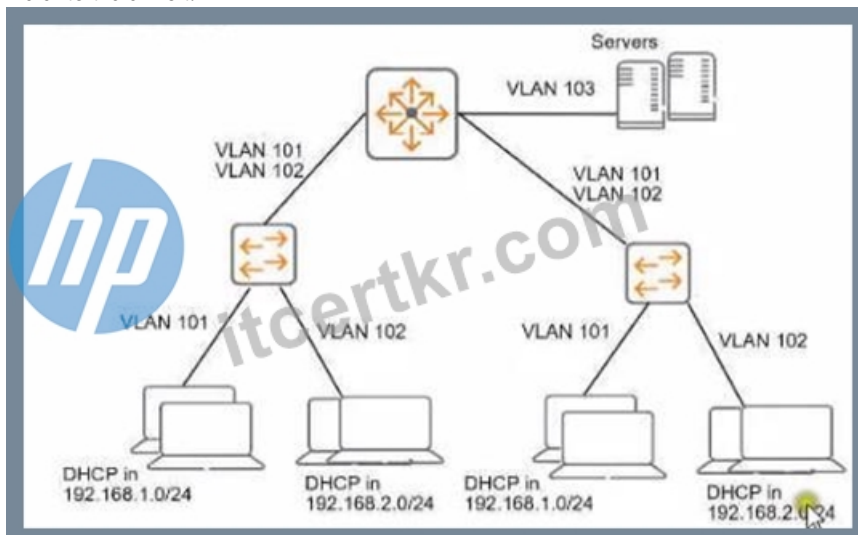
You need to ensure that only management stations in subnet 192.168.1.0/24 can access the ArubaOS-Switches' CLI. Web Ul. and

REST interfaces The company also wants to let managers use these stations to access other parts of the network What should you do?

- A. Establish a Control Plane Policing class that selects traffic from 192.168 1.0/24.
- B. Configure the switch to listen for these protocols on OOBM only.
- C. Specify vlan 100 as the management vlan for the switches.
- D. Specify 192.168.1.0.255.255.255.0 as authorized IP manager address

정답：A

질문 # 123

What is a benefit of Protected Management Frames (PMF). sometimes called Management Frame Protection (MFP)?

- A. PMF helps to protect APs and MCs from unauthorized management access by hackers.
- B. PMF ensures trial traffic between APs and Mobility Controllers (MCs) is encrypted.
- C. PMF protects clients from DoS attacks based on forged de-authentication frames
- D. PMF prevents hackers from capturing the traffic between APs and Mobility Controllers.

정답：C

설명：
Protected Management Frames (PMF), also known as Management Frame Protection (MFP), is designed to protect clients from denial-of-service (DoS) attacks that involve forged de-authentication and disassociation frames. These attacks can disconnect legitimate clients from the network. PMF provides a way to authenticate these management frames, ensuring that they are not forged, thus enhancing the security of the wireless network.
:
IEEE 802.11w amendment, which introduces PMF as a security enhancement to protect management frames.
Wi-Fi Alliance security guidelines for Protected Management Frames (PMF).

질문 # 124

What is one way that Control Plane Security (CPsec) enhances security for me network?

- A. It protects management traffic between APs and Mobility Controllers (MCs) from eavesdropping.
- B. It prevents access from unauthorized IP addresses to critical services, such as SSH on Mobility Controllers (MCs).
- C. It prevents Denial of Service (DoS) attacks against Mobility Controllers' (MCs") control plane.
- D. It protects wireless clients' traffic tunneled between APs and Mobility Controllers, from eavesdropping

정답：A

설명：
Control Plane Security (CPsec) enhances security in the network by protecting management traffic between APs and Mobility Controllers (MCs) from eavesdropping. CPsec ensures that all control and management traffic that transits the network is encrypted, thus preventing potential attackers from gaining access to sensitive management data. It helps in securing the network's control plane, which is crucial for maintaining the integrity and privacy of the network operations.References:
Aruba Networks' CPsec documentation.

질문 # 125

What is one difference between EAP-Tunneled Layer Security (EAP-TLS) and Protected EAP (PEAP)?

- A. EAP-TLS creates a TLS tunnel for transmitting user credentials, while PEAP authenticates the server and supplicant during a TLS handshake.
- B. EAP-TLS requires the supplicant to authenticate with a certificate, but PEAP allows the supplicant to use a username and password.
- C. EAP-TLS creates a TLS tunnel for transmitting user credentials securely, while PEAP protects user credentials with TKIP encryption.
- D. EAP-TLS begins with the establishment of a TLS tunnel, but PEAP does not use a TLS tunnel as part of its process.

정답：B

설명：

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) and PEAP (Protected EAP) are two EAP methods used for 802.1X authentication in wireless networks, such as those configured with WPA3-Enterprise on HPE Aruba Networking solutions. Both methods are commonly used with ClearPass Policy Manager (CPPM) for secure authentication.

EAP-TLS:

Requires both the supplicant (client) and the server (e.g., CPPM) to present a valid certificate during authentication.

Establishes a TLS tunnel to secure the authentication process, but the primary authentication mechanism is the mutual certificate exchange. The client's certificate is used to authenticate the client, and the server's certificate authenticates the server.

PEAP:

Requires only the server to present a certificate to authenticate itself to the client.

Establishes a TLS tunnel to secure the authentication process, within which the client authenticates using a secondary method, typically a username and password (e.g., via MS-CHAPv2 or EAP-GTC).

Option A, "EAP-TLS begins with the establishment of a TLS tunnel, but PEAP does not use a TLS tunnel as part of its process," is incorrect. Both EAP-TLS and PEAP establish a TLS tunnel. In EAP-TLS, the TLS tunnel is used for the mutual certificate exchange, while in PEAP, the TLS tunnel protects the inner authentication (e.g., username/password).

Option B, "EAP-TLS requires the supplicant to authenticate with a certificate, but PEAP allows the supplicant to use a username and password," is correct. This is a key difference: EAP-TLS mandates certificate-based authentication for the client, while PEAP allows the client to authenticate with a username and password inside the TLS tunnel, making PEAP more flexible for environments where client certificates are not deployed.

Option C, "EAP-TLS creates a TLS tunnel for transmitting user credentials, while PEAP authenticates the server and supplicant during a TLS handshake," is incorrect. Both methods use a TLS tunnel, and both authenticate the server during the TLS handshake (using the server's certificate). In EAP-TLS, the client's certificate is also part of the TLS handshake, while in PEAP, the client's credentials (username/password) are sent inside the tunnel after the handshake.

Option D, "EAP-TLS creates a TLS tunnel for transmitting user credentials securely, while PEAP protects user credentials with TKIP encryption," is incorrect. PEAP does not use TKIP (Temporal Key Integrity Protocol) for protecting credentials; TKIP is a legacy encryption method used in WPA/WPA2 for wireless data encryption, not for EAP authentication. PEAP uses the TLS tunnel to protect the inner authentication credentials.

The HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide states:

"EAP-TLS requires both the supplicant and the server to present a valid certificate for mutual authentication. The supplicant authenticates using its certificate, and the process is secured within a TLS tunnel. In contrast, PEAP requires only the server to present a certificate to establish a TLS tunnel, within which the supplicant can authenticate using a username and password (e.g., via MS-CHAPv2 or EAP-GTC). This makes PEAP more suitable for environments where client certificates are not deployed." (Page 292, EAP Methods Section) Additionally, the HPE Aruba Networking Wireless Security Guide notes:

"A key difference between EAP-TLS and PEAP is the client authentication method. EAP-TLS mandates that the client authenticate with a certificate, requiring certificate deployment on all clients. PEAP allows the client to authenticate with a username and password inside a TLS tunnel, making it easier to deploy in environments without client certificates." (Page 40, 802.1X Authentication Methods Section)

:

HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, EAP Methods Section, Page 292.

HPE Aruba Networking Wireless Security Guide, 802.1X Authentication Methods Section, Page 40.

질문 # 126

......

HPE6-A78인기덤프문제: https://www.itcertkr.com/HPE6-A78_exam.html

그리고 Itcertkr HPE6-A78 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다:
https://drive.google.com/open?id=1apW65ZTL8T11wMEX6caL_79dbscdlTX8