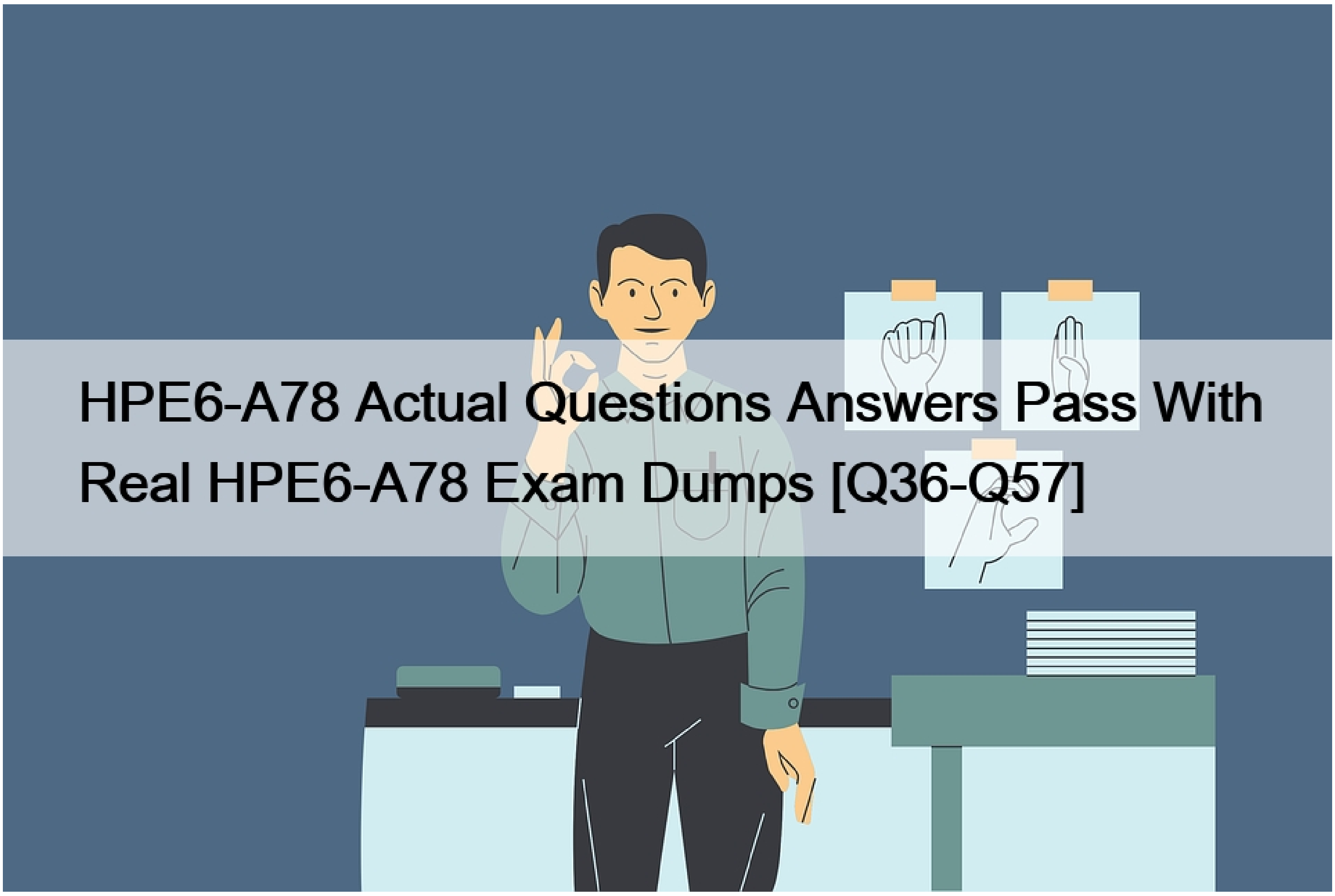
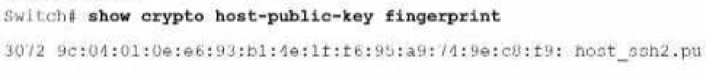
HPE6-A78 Actual Questions Answers Pass With Real HPE6-A78 Exam Dumps [Q36-Q57



HPE6-A78 Actual Questions Answers Pass With Real HPE6-A78 Exam Dumps HPE6-A78 Dumps Prepare Your Exam With 62 Questions QUESTION 36

Refer to the exhibit.



```
Switch# show crypto host-public-key fingerprint
3072 9c:04:01:0e:e6:93:b1:4e:1f:f6:95:a9:74:9e:c8:f9: host_ssh2.pu
```

How can you use the thumbprint?
* Install this thumbprint on management stations to use as two-factor authentication along with manager usernames and passwords, this will ensure managers connect from valid stations
* Copy the thumbprint to other Aruba switches to establish a consistent SSH Key for all switches this will enable managers to connect to the switches securely with less effort
* When you first connect to the switch with SSH from a management station, make sure that the thumbprint matches to ensure that a man-in-t he-mid die (MITM) attack is not occurring

* install this thumbprint on management stations the stations can then authenticate with the thumbprint instead of admins having to enter usernames and passwords.

QUESTION 37

What is a benefit or using network aliases in ArubaOS firewall policies?
* You can associate a reputation score with the network alias to create rules that filler traffic based on reputation rather than IP.
* You can use the aliases to translate client IP addresses to other IP addresses on the other side of the firewall
* You can adjust the IP addresses in the aliases, and the rules using those aliases automatically update
* You can use the aliases to conceal the true IP addresses of servers from potentially untrusted clients.

QUESTION 38

What correctly describes the Pairwise Master Key (PMK) in thee specified wireless security protocol?
* In WPA3-Enterprise, the PMK is unique per session and derived using Simultaneous Authentication of Equals.
* In WPA3-Personal, the PMK is unique per session and derived using Simultaneous Authentication of Equals.
* In WPA3-Personal, the PMK is derived directly from the passphrase and is the same tor every session.
* In WPA3-Personal, the PMK is the same for each session and is communicated to clients that authenticate

QUESTION 39

An ArubaOS-CX switch enforces 802.1X on a port. No fan-through options or port-access roles are configured on the port The 802 1X supplicant on a connected client has not yet completed authentication Which type of traffic does the authenticator accept from the client?
* EAP only
* DHCP, DNS and RADIUS only
* RADIUS only
* DHCP, DNS, and EAP only

QUESTION 40

What is a correct guideline for the management protocols that you should use on ArubaOS-Switches?
* Disable Telnet and use TFTP instead.
* Disable SSH and use https instead.
* Disable Telnet and use SSH instead
* Disable HTTPS and use SSH instead

QUESTION 41

What is a vulnerability of an unauthenticated Dime-Heliman exchange?
* A hacker can replace the public values exchanged by the legitimate peers and launch an MITM attack.
* A brute force attack can relatively quickly derive Diffie-Hellman private values if they are able to obtain public values
* Diffie-Hellman with elliptic curve values is no longer considered secure in modem networks, based on NIST recommendations.
* Participants must agree on a passphrase in advance, which can limit the usefulness of Diffie- Hell man in practical contexts.

QUESTION 42

What is an Authorized client as defined by ArubaOS Wireless Intrusion Prevention System (WIP)?
* a client that has a certificate issued by a trusted Certification Authority (CA)
* a client that is not on the WIP blacklist

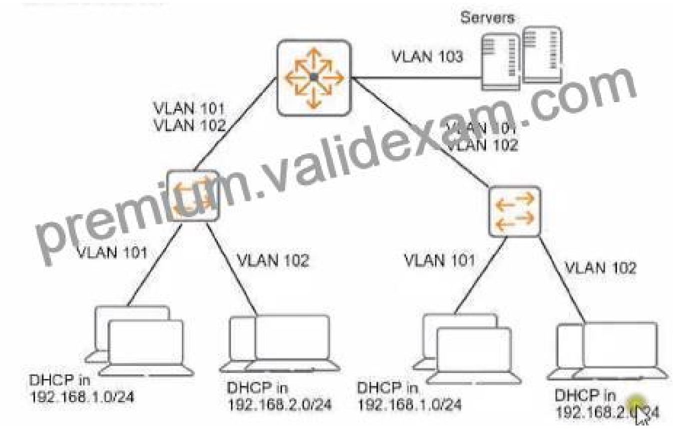
* a client that has successfully authenticated to an authorized AP and passed encrypted traffic
* a client that is on the WIP whitelist.

QUESTION 43

What is a Key feature of me ArubaOS firewall?
* The firewall is stateful which means that n can track client sessions and automatically allow return traffic for permitted sessions
* The firewall Includes application layer gateways (ALGs). which it uses to filter Web traffic based on the reputation of the destination web site.
* The firewall examines all traffic at Layer 2 through Layer 4 and uses source IP addresses as the primary way to determine how to control traffic.
* The firewall is designed to fitter traffic primarily based on wireless 802.11 headers, making it ideal for mobility environments

QUESTION 44

Refer to the exhibit.



You need to ensure that only management stations in subnet 192.168.1.0/24 can access the ArubaOS-Switches&#8217; 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?
* Establish a Control Plane Policing class that selects traffic from 192.168 1.0/24.
* Specify 192.168.1.0.255.255.255.0 as authorized IP manager address
* Configure the switch to listen for these protocols on OOBM only.
* Specify vlan 100 as the management vlan for the switches.

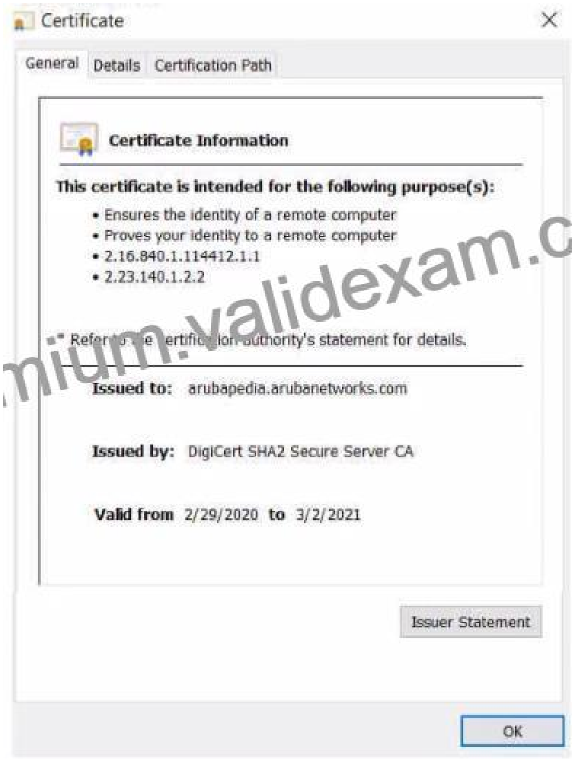
QUESTION 45

You are configuring ArubaOS-CX switches to tunnel client traffic to an Aruba Mobility Controller (MC).

What should you do to enhance security for control channel communications between the switches and the MC?
* Create one UBT zone for control traffic and a second UBT zone for clients.
* Configure a long, random PAPI security key that matches on the switches and the MC.
* install certificates on the switches, and make sure that CPsec is enabled on the MC
* Make sure that the UBT client vlan is assigned to the interface on which the switches reach the MC and only that interface.

QUESTION 46

Refer to the exhibit.



This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: arubapedia.arubanetworks.com

Issued by: DigiCert SHA2 Secure Server CA

Valid from 2/29/2020 **to** 3/2/2021

Device A is establishing an HTTPS session with the Arubapedia web sue using Chrome. The Arubapedia web server sends the certificate shown in the exhibit What does the browser do as part of vacating the web server certificate?
* It uses the public key in the DigCen SHA2 Secure Server CA certificate to check the certificate&#8217;s signature.
* It uses the public key in the DigCert root CA certificate to check the certificate signature
* It uses the private key in the DigiCert SHA2 Secure Server CA to check the certificate&#8217;s signature.
* It uses the private key in the Arubapedia web site&#8217;s certificate to check that certificate&#8217;s signature

QUESTION 47

You are managing an Aruba Mobility Controller (MC). What is a reason for adding a &#8220;Log Settings&#8221; definition in the ArubaOS Diagnostics > System > Log Settings page?
* Configuring the Syslog server settings for the server to which the MC forwards logs for a particular category and level
* Configuring the MC to generate logs for a particular event category and level, but only for a specific user or AP.
* Configuring a filter that you can apply to a defined Syslog server in order to filter events by subcategory
* Configuring the log facility and log format that the MC will use for forwarding logs to all Syslog servers

QUESTION 48

What is one way that WPA3-PerSonal enhances security when compared to WPA2-Personal?
* WPA3-Perscn3i is more secure against password leaking Because all users nave their own username and password
* WPA3-Personai prevents eavesdropping on other users&#8217; wireless traffic by a user who knows the passphrase for the WLAN.
* WPA3-Personai is more resistant to passphrase cracking Because it requires passphrases to be at least 12 characters

* WPA3-Personal is more complicated to deploy because it requires a backend authentication server

QUESTION 49

Which is a correct description of a stage in the Lockheed Martin kill chain?
* In the delivery stage, malware collects valuable data and delivers or exfilltrated it to the hacker.
* In the reconnaissance stage, the hacker assesses the impact of the attack and how much information was exfilltrated.
* In the weaponization stage, which occurs after malware has been delivered to a system, the malware executes Its function.
* In the exploitation and installation phases, malware creates a backdoor into the infected system for the hacker.

QUESTION 50

Your ArubaoS solution has detected a rogue AP with Wireless intrusion Prevention (WIP). Which information about the detected radio can best help you to locate the rogue device?
* the match method
* the detecting devices
* the match type
* the confidence level

QUESTION 51

What role does the Aruba ClearPass Device Insight Analyzer play in the Device Insight architecture?
* It resides in the cloud and manages licensing and configuration for Collectors
* It resides on-prem and provides the span port to which traffic is mirrored for deep analytics.
* It resides on-prem and is responsible for running active SNMP and Nmap scans
* It resides In the cloud and applies machine learning and supervised crowdsourcing to metadata sent by Collectors

QUESTION 52

What are the roles of 802.1X authenticators and authentication servers?
* The authenticator stores the user account database, while the server stores access policies.
* The authenticator supports only EAP, while the authentication server supports only RADIUS.
* The authenticator is a RADIUS client and the authentication server is a RADIUS server.
* The authenticator makes access decisions and the server communicates them to the supplicant.

QUESTION 53

What is a guideline for managing local certificates on an ArubaOS-Switch?
* Before installing the local certificate, create a trust anchor (TA) profile with the root CA certificate for the certificate that you will install
* Install an Online Certificate Status Protocol (OCSP) certificate to simplify the process of enrolling and re-enrolling for certificate
* Generate the certificate signing request (CSR) with a program offline, then, install both the certificate and the private key on the switch in a single file.
* Create a self-signed certificate online on the switch because ArubaOS-Switches do not support CA-signed certificates.

QUESTION 54

What is one way that Control Plane Security (CPsec) enhances security for me network?
* It protects wireless clients&#8217; traffic tunneled between APs and Mobility Controllers, from eavesdropping
* It prevents Denial of Service (DoS) attacks against Mobility Controllers&#8217; (MCs&#8221;) control plane.

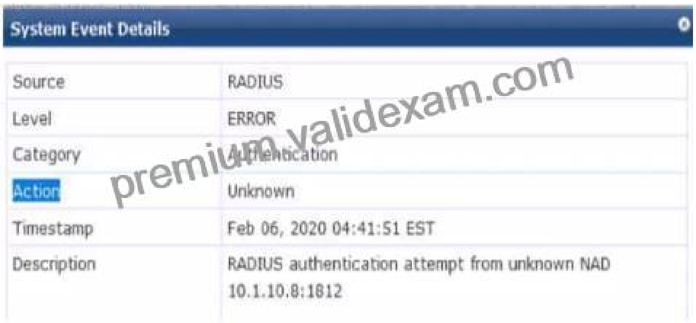
* It prevents access from unauthorized IP addresses to critical services, such as SSH on Mobility Controllers (MCs).
* It protects management traffic between APs and Mobility Controllers (MCs) from eavesdropping.

QUESTION 55

What is a benefit of deploying Aruba ClearPass Device insight?
* Highly accurate endpoint classification for environments with many devices types, including Internet of Things (loT)
* visibility into devices&#8217; 802.1X supplicant settings and automated certificate deployment
* Agent-based analysts of devices&#8217; security settings and health status, with the ability to implement quarantining
* Simpler troubleshooting of ClearPass solutions across an environment with multiple ClearPass Policy Managers

QUESTION 56

Refer to the exhibit.



System Event Details

Source	RADIUS
Level	ERROR
Category	Authentication
Action	Unknown
Timestamp	Feb 06, 2020 04:41:51 EST
Description	RADIUS authentication attempt from unknown NAD 10.1.10.8:1812

You are deploying a new ArubaOS Mobility Controller (MC), which is enforcing authentication to Aruba ClearPass Policy Manager (CPPM). The authentication is not working correctly, and you find the error shown In the exhibit in the CPPM Event Viewer.

What should you check?
* that the MC has been added as a domain machine on the Active Directory domain with which CPPM is synchronized
* that the snared secret configured for the CPPM authentication server matches the one defined for the device on CPPM
* that the IP address that the MC is using to reach CPPM matches the one defined for the device on CPPM
* that the MC has valid admin credentials configured on it for logging into the CPPM

QUESTION 57

Your Aruba Mobility Master-based solution has detected a rogue AP Among other information the ArubaOS Detected Radios page lists this Information for the AP SSID = PubllcWiFI BSSID = a8M27 12 34:56 Match method = Exact match Match type = Eth-GW-wired-Mac-Table The security team asks you to explain why this AP is classified as a rogue. What should you explain?
* The AP Is connected to your LAN because It is transmitting wireless traffic with your network&#8217;s default gateway&#8217;s MAC address as a source MAC Because it does not belong to the company, it is a rogue
* The ap has a BSSID mat matches authorized client MAC addresses. This indicates that the AP is spoofing the MAC address to gam unauthorized access to your company&#8217;s wireless services, so It is a rogue
* The AP has been detected as launching a DoS attack against your company&#8217;s default gateway. This qualities it as a rogue which needs to be contained with wireless association frames immediately
* The AP is spoofing a routers MAC address as its BSSID. This indicates mat, even though WIP cannot determine whether the AP is connected to your LAN. it is a rogue.

New HPE6-A78 Dumps - Real HP Exam Questions: https://www.validexam.com/HPE6-A78-latest-dumps.html]