100% Pass Quiz HP Latest HPE7-A02 Reliable Test Cram

2026 Latest Itcertkey HPE7-A02 PDF Dumps and HPE7-A02 Exam Engine Free Share: https://drive.google.com/open?id=1Abx3zRBlu_R7I4V4Se42HigUWOzygv9B

The accuracy rate of Itcertkey HPE7-A02 exam certification training materials is high with wide coverage. It not only can improve your cultural knowledge, but also improve your operation level. It not only makes you become IT elite, but also make you have a well-paid job that others admire. Before buying our HPE7-A02 Certification Training materials, you can download HPE7-A02 free demo and answers on probation on Itcertkey website.

HPE7-A02 exam covers a wide range of topics related to network security. These include securing wireless and wired networks, implementing firewalls and intrusion prevention systems, managing network access control, and detecting and responding to security incidents. HPE7-A02 Exam also covers key concepts such as risk management, regulatory compliance, and security best practices.

>> HPE7-A02 Reliable Test Cram <<

HP Realistic HPE7-A02 Reliable Test Cram Free PDF Quiz

You can open the HP PDF questions file from any location and go through actual HPE7-A02 exam questions without time restrictions. The Aruba Certified Network Security Professional Exam HPE7-A02 practice test is ideal for intensive preparation. You can attempt our Aruba Certified Network Security Professional Exam HPE7-A02 Practice Exam multiple times to review and enhance your test preparation. The real HPE7-A02 exam environment of desktop and web-based practice exams will help you counter Aruba Certified Network Security Professional Exam HPE7-A02 pass anxiety.

HP HPE7-A02 Certification Exam is an excellent way for IT professionals to demonstrate their knowledge and skills in network security using Aruba products. By obtaining this certification, candidates can enhance their career prospects and demonstrate their proficiency in implementing and managing secure networks using Aruba products.

HP Aruba Certified Network Security Professional Exam Sample Questions (Q19-Q24):

NEW QUESTION # 19
You are configuring the HPE Aruba Networking ClearPass Device Insight Integration settings on ClearPass Policy Manager (CPPM). For which use case should you set the 'Tag Updates Action" to " apply for all tag updates"?

- A. When Device Insight tags are only used to identify dangerous devices, and you want to disconnect those devices without having to set up new rules in enforcement policies.
- B. When the Device Insight integration poll interval is set to a relatively long interval but you still want CPPM to be informed quickly about devices' new tags.
- C. When you plan to have CPPM issue CoAs for clients with new tags, but do not want to have to list those specific tags in the Device Integration settings in advance.

- D. When CPPM is gathering posture information for CPDI, and you want CPDI to always have access to the most up-to-date information.

Answer: C

Explanation:
* Tag Updates Action - "Apply for All Tag Updates":
* This setting ensures that all updated tags from Device Insight (CPDI) are applied dynamically.
* It is particularly useful when you want to trigger Change of Authorization (CoA) without explicitly predefining the tag values.
* Option D: Correct. This setting allows CPPM to issue CoAs automatically for updated tags without requiring prior configuration of specific tags.
* Option A: Incorrect. The setting is not directly related to reducing the poll interval latency.
* Option B: Incorrect. Disconnecting devices based on dangerous tags would require predefined enforcement rules.
* Option C: Incorrect. Posture information updates do not directly rely on this setting.

NEW QUESTION # 20
A company has been running Gateway IDS/IPS on its gateways in IDS mode for several weeks. The company wants to transition to IPS mode.
What is one step you should recommend?

- A. Check for legitimate traffic that has been flagged as a threat and allow list the associated rules.
- B. Disable traffic inspection and reboot before re-enabling traffic inspection with the new mode.
- C. Change the mode on one gateway at a time to establish a smoother transition period.
- D. Consider applying a stricter IPS policy to minimize issues during the transition period.

Answer: A

Explanation:
When transitioning from Intrusion Detection System (IDS) mode to Intrusion Prevention System (IPS) mode, it's critical to review and refine configurations to ensure legitimate traffic is not blocked. Here's the reasoning behind each option:
A: Disable traffic inspection and reboot before re-enabling traffic inspection with the new mode.
* Incorrect:
* Transitioning to IPS mode does not require a full reboot or disabling traffic inspection.
* This step is unnecessary and could lead to downtime that impacts network operations.
B: Change the mode on one gateway at a time to establish a smoother transition period.
* Incorrect:
* While a phased approach might help in some large deployments, it does not directly address the potential for legitimate traffic to be blocked by IPS mode.
* IPS operates in real-time, so misconfigured rules or policies need to be addressed before enabling IPS on any gateway.
C: Consider applying a stricter IPS policy to minimize issues during the transition period.
* Incorrect:
* A stricter IPS policy increases the likelihood of false positives, which could disrupt legitimate business-critical traffic.
* During the transition, the focus should be on minimizing disruptions by fine-tuning policies, not making them stricter.
D: Check for legitimate traffic that has been flagged as a threat and allow list the associated rules.
* Correct:
* In IDS mode, the system only detects and logs suspicious traffic but does not block it. Reviewing these logs for false positives allows the organization to fine-tune policies and allow list legitimate traffic before transitioning to IPS mode.
* By doing this, the company ensures that IPS mode will block actual threats while permitting legitimate traffic.
* This is a proactive step to prevent unnecessary disruptions to normal operations when IPS mode is enabled.
References
* HPE Aruba Gateway IDS/IPS Configuration Guide.
* Best Practices for Transitioning from IDS to IPS Modes in Aruba Networks.
* Aruba Network Threat Management Documentation.

NEW QUESTION # 21
A company uses HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application option). In the details for a generic device cluster, you see a recommendation for "Windows 8/10" with 70% accuracy.
What does this mean?

- A. CPDI has detected that these devices match about 70% of the system rule for defining "Windows 8/10" devices.
- B. CPDI has matched these devices against several, conflicting system rules. 70% of those rules are for "Windows 8/10" devices.
- C. CPDI has used MAC OUI to group these devices together. The average device's MAC address matches 70% of the "Windows 8/10" OUI.
- D. CPDI has grouped this cluster with similar classified devices. 70% of those classified devices are "Windows 8/10."

Answer: A

Explanation:
When HPE Aruba Networking ClearPass Device Insight (CPDI) shows a recommendation for "Windows 8/10" with 70% accuracy for a generic device cluster, it means that CPDI has detected that these devices match about 70% of the system rule criteria for defining "Windows 8/10" devices. This percentage indicates the confidence level based on the observed characteristics and behavior of the devices, helping administrators understand the likelihood that these devices are indeed running Windows 8 or 10.

NEW QUESTION # 22
The following firewall role is configured on HPE Aruba Networking Central-managed APs:
wlan access-rule employees
index 3
rule any any match 17 67 67 permit
rule any any match any 53 53 permit
rule 10 5 5.0 255.255 255.0 match any any any deny
rule 10.5 0.0 255.255 0.0 match 6 80 80 permit
rule 10.5 0.0 255.255.0.0 match 6 443 443 permit
rule 10.5.0.0 255.255.0.0 match any any any deny
rule any any match any any any permit
A client has authenticated and been assigned to the employees role. The client has IP address 10.2.2.2. Which correctly describes behavior in this policy?

- A. Traffic from 198.51.100.12 in an active HTTP session between 10.2.2.2 and 198.51.100.12 is denied.
- B. HTTPS traffic from 10.2.2.2 to 10.5.5.5 is denied.
- C. HTTPS traffic from 10.2.2.2 to 203.0.113.12 is denied.
- D. Traffic from 10.5.3.3 in an active HTTPS session between 10.2.2.2 and 10.5.3.3 is permitted.

Answer: B

Explanation:
* Policy Analysis:
* Rule Evaluation Order: Rules are applied in sequential order until a match is found.
* Key Points:
* DHCP traffic (UDP 67) is permitted.
* DNS traffic (UDP 53) is permitted.
* Traffic to 10.5.5.0/24 is explicitly denied.
* HTTP traffic (TCP 80) is allowed only to 10.5.0.0/16.
* HTTPS traffic (TCP 443) is allowed only to 10.5.0.0/16.
* All other traffic to 10.5.0.0/16 is denied.
* Any other traffic not matching the above rules is permitted.
* Scenario Analysis:
* The client IP 10.2.2.2 does not fall within the 10.5.0.0/16 subnet.
* Rule 3 denies traffic to 10.5.5.5, regardless of the source IP.
* Option A: Correct. HTTPS traffic to 10.5.5.5 is explicitly denied by Rule 3.
* Option B: Incorrect. Traffic to 203.0.113.12 is permitted due to the final "permit any" rule.
* Option C: Incorrect. The client (10.2.2.2) does not belong to the subnet 10.5.0.0/16, so traffic to 10.5.3.3 is not permitted by Rule 5.
* Option D: Incorrect. HTTP traffic to 198.51.100.12 is allowed by the last "permit any" rule.

NEW QUESTION # 23

A company lacks visibility into the many different types of user and loT devices deployed in its internal network, making it hard for the security team to address those devices.
Which HPE Aruba Networking solution should you recommend to resolve this issue?

- A. HPE Aruba Networking ClearPass OnBoard
- B. HPE Aruba Networking ClearPass Device Insight (CPDI)
- C. HPE Aruba Networking Network Analytics Engine (NAE)
- D. HPE Aruba Networking Mobility Conductor

Answer: B

Explanation:
For a company that lacks visibility into various types of user and IoT devices on its internal network, HPE Aruba Networking ClearPass Device Insight (CPDI) is the recommended solution. CPDI provides comprehensive visibility and profiling of all devices connected to the network. It uses machine learning and AI to identify and classify devices, offering detailed insights into their behavior and characteristics. This enhanced visibility enables the security team to effectively monitor and manage network devices, improving overall network security and compliance.

NEW QUESTION # 24
......

id=1Abx3zRBlu_R7I4V4Se42HigUWOzygv9B