Question #1 *Topic 1*

A company uses HPE Networking ClearPass Policy Manager (CPPM) as a TACACS+ server to authenticate managers on its AOS-CX switches. The company wants CPPM to control commands managers are allowed to enter.
Which service must you add to the managers' TACACS+ enforcement profile?

A. Cpass: HTTP

B. Shell

C. ARAP

D. Aruba:Common

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

An AOS-CX switch has this admin user account configured on it: netadmin in the operators group

You have configured these commands on an AOS-CX switch:

tacacs-server host cp.example.com key plaintext &12xl.powmay7855 aaa authentication login ssh group tacacs local aaa authentication allow-fail-through

A user accesses the switch with SSH and logs in as netadmin with the correct password. When switch sends a TACACS+ request to the ClearPass server at cp.example.com, the server does not send a response. Authentication times out.

What happens?

A. The user is logged in and granted operator access.

B. The user is logged in and allowed to enter auditor commands only.

C. The user is logged in and granted administrators access.

D. The user is not allowed to log in.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

You have created this rule in an HPE Aruba Networking ClearPass Policy Manager (CPPM) service's enforcement policy. IF Authorization [Endpoints Repository] Conflict EQUALS true THEN apply "quarantine_profile"
What information can help you determine whether you need to configure cluster-wide profiler parameters to ignore some conflicts?

A. Whether the company has devices that use PXE boot

B. Whether some devices are incapable of captive portal or 802.1X authentication

C. Whether the company has rare Internet of Things (IoT) devices

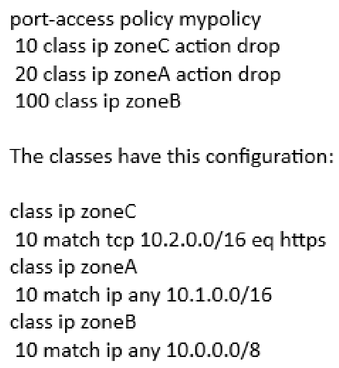
D. Whether some devices are running legacy operating systems

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

A port-access role for AOS-CX switches has this policy applied to it:



```
port-access policy mypolicy
 10 class ip zoneC action drop
 20 class ip zoneA action drop
 100 class ip zoneB
```

The classes have this configuration:

```
class ip zoneC
 10 match tcp 10.2.0.0/16 eq https
class ip zoneA
 10 match ip any 10.1.0.0/16
class ip zoneB
 10 match ip any 10.0.0.0/8
```

The company wants to permit clients in this role to access 10.2.12.0/24 with HTTPS.

What should you do?

A. Add this rule to zoneC: 5 match any 10.2.12.0/24 eq https

B. Add this rule to zone A: 5 ignore tcp any 10.2.12.0/24 eq https

C. Add this rule to zone B: 5 match tcp any 10.2.12.0/24 eq https

D. Add this rule to zoneC: 5 ignore tcp any 10.2.12.0/24 eq https

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

You are setting up HPE Aruba Networking SSE to prohibit users from uploading and downloading files from Dropbox. What is part of the process?

A. adding a web category that includes Dropbox

B. installing the HPE Aruba Networking SSE root certificate on clients

C. deploying a connector that can reach the remote users

D. deploying a connector that can reach Dropbox

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

You are setting up user based tunneling (UBT) between access layer AOS-CX switches and AOS-10 gateways. You have selected reserved (local) VLAN mode.
Tunneled devices include IoT devices, which should be assigned to:
*Roles: iot on the switches and iot-wired on the gateways
*VLAN: 64, for which the gateways route traffic
IoT devices connect to the access layer switches' edge ports, and the access layer switches reach the gateways on their uplinks.
Where must you configure VLAN 64?

A. In the iot-wired role and on no physical interfaces

B. In the iot role and the iot-wired role and on no physical interfaces

C. In the iot-wired role and the access switch uplinks

D. In the iot role and the access switch uplinks

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

A company has a third-party security appliance deployed in its data center. The company wants to pass all traffic for certain clients through that device before forwarding that traffic toward its ultimate destination.
Which AOS-CX switch technology fulfills this use case?

A. Virtual Network Based Tunneling (VNBT)

B. MC-LAG

C. Network Analytics Engine (NAE)

D. Device profiles

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

You manage AOS-10 APs with HPE Aruba Networking Central. A role is configured on these APs with these rules:

1. Allow udp on port 67 to any destination
2. Allow any to network 10.1.6.0/23
3. Deny any to network 10.1.0.0/16 + log
4. Deny any to network 10.0.0.0/8
5. Allow any to any destination

You add this new rule immediately before rule 2:

Deny ssh to network 10.1.4.0/23 + denylist

After this change, what happens when a client assigned to this role sends SSH traffic to 10.1.11.42?

A. The traffic is permitted.

B. The traffic is dropped and logged.

C. The traffic is dropped (without any logging or further action against the client).

D. The traffic is dropped, and the client is denylisted.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

HPE Aruba Networking ClearPass Device Insight (CPDI) could not classify some endpoints using system and user rules. Using machine learning, it did assign those endpoints to a cluster and discover a recommendation. In which of these circumstances does CPDI automatically classify the endpoints based on that recommendation?

A. The recommendation has 96% confidence, and it based on 13 classified devices.

B. The recommendation has 98% confidence, and it based on 5 classified devices.

C. The recommendation has 93% confidence, and it based on 36 classified devices.

D. The recommendation has 100% confidence, and it based on 4 classified devices.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

You are setting up HPE Aruba Networking SSE. Which use case requires you to apply a non-default posture in a rule?

A. applying threat inspection to users when they access certain web sites

B. checking whether a client has antivirus software as a condition for receiving access to resources

C. redirecting compromised clients to a remediation server

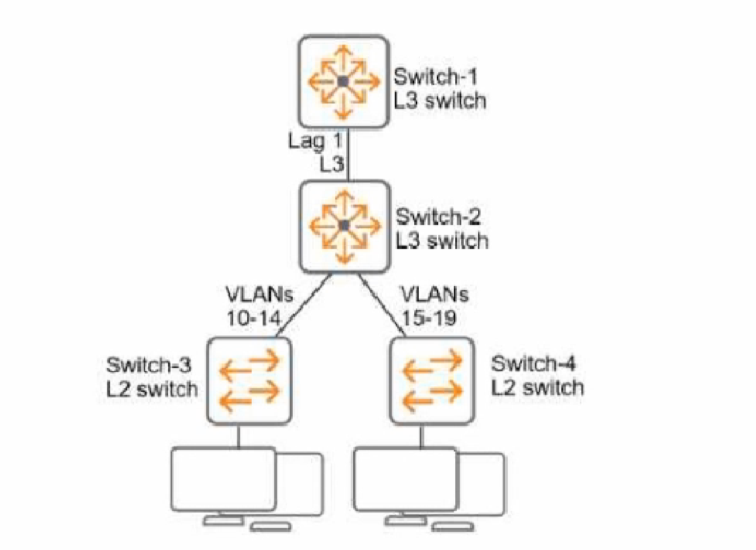
D. integrating with HPE Aruba Networking ClearPass OnGuard

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Refer to the exhibit.



All of the switches in the exhibit are AOS-CX switches.

What is the preferred configuration on Switch-2 for preventing rogue OSPF routers in this network?

A. Configure OSPF authentication on VLANs 10-19 is password mode.

B. Configure OSPF authentication on Lag 1 in MD5 mode.

C. Disable OSPF entirely on VLANs 10-19.

D. Configure passive-interface as the OSPF default and disable OSPF passive on Lag 1.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Which issue can an HPE Aruba Networking Secure Web Gateway (SWG) solution help customers address?

A. The organization needs a faster way to quarantine clients that have generated threats, as detected by third-party firewalls.

B. Hybrid workers are exposing their computers to risky internet sites and infection by malware when they work from home.

C. Remote workers need access to private data center applications without exposing those applications to unauthorized users.

D. The organization currently has no way to prevent users from exfiltrating sensitive data from SaaS applications.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

A company has several use cases for using its AOS-CX switches’ HPE Aruba Networking Analytics Engine (NAE).
What is one guideline to keep in mind as you plan?

A. Each switch model has a maximum number of supported monitors, and one agent might have multiple monitors.

B. You can install multiple scripts on a switch, but you can deploy only one agent per script.

C. The switch will permit you to deploy as many NAE agents as you want, but they might degrade the switch functionality.

D. When you use custom scripts, you can create as many agents from each script as you want.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

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. Disable traffic inspection and reboot before re-enabling traffic inspection with the new mode.

B. Change the mode on one gateway at a time to establish a smoother transition period.

C. Consider applying a stricter IPS policy to minimize issues during the transition period.

D. Check for legitimate traffic that has been flagged as a threat and allow list the associated rules.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #15

Topic 1

A ClearPass Policy Manager (CPPM) service includes these settings:
Role mapping policy:

Evaluate: Select first -
Rule 1 conditions: Authorization:AD:Groups EQUALS Managers AND Authentication:TEAP-Method-1-Status EQUALS Success

Rule 1 role: manager -
Rule 2 conditions: Authentication:TEAP-Method-1-Status EQUALS Success

Rule 2 role: domain-comp -
Default role: [Other]
Enforcement policy:

Evaluate: Select first -
Rule 1 conditions: Tips Role EQUALS manager AND Tips Role EQUALS domain-comp
Rule 1 profile list: domain-manager
Rule 2 conditions: Tips Role EQUALS manager
Rule 2 profile list: manager-only
Rule 3 conditions: Tips Role EQUALS domain-comp
Rule 3 profile list: domain-only
Default profile: [Deny access]
A client is authenticated by the service. CPPM collects attributes indicating that the user is in the Contractors group, and the client passed both TEAP methods.
Which enforcement policy will be applied?

A. [Deny Access Profile]

B. manager-only

C. domain-manager

D. domain-only

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

A company has HPE Aruba Networking APs managed by HPE Aruba Networking Central. You have set up a WLAN to enforce WPA3 with 802.1X authentication.
What happens if the client fails authentication?

A. The AP assigns the client to the WLAN's default role.

B. The AP drops the client because authentication aborts.

C. The AP assigns the client to the WLAN's critical role.

D. The AP assigns the client to the WLAN's initial role.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

A company wants you to integrate HPE Aruba Networking ClearPass Policy Manager (CPPM) with HPE Aruba Networking ClearPass Device Insight (CPDI).
What is one aspect of the integration that you should explain?

A. CPPM no longer supports any Device Profiler features and relies on CPDI for this profile information.

B. CPDI must be configured as an audit server on CPPM for the integration to be successful.

C. CPDI must have security analysis disabled on it for the integration to be successful.

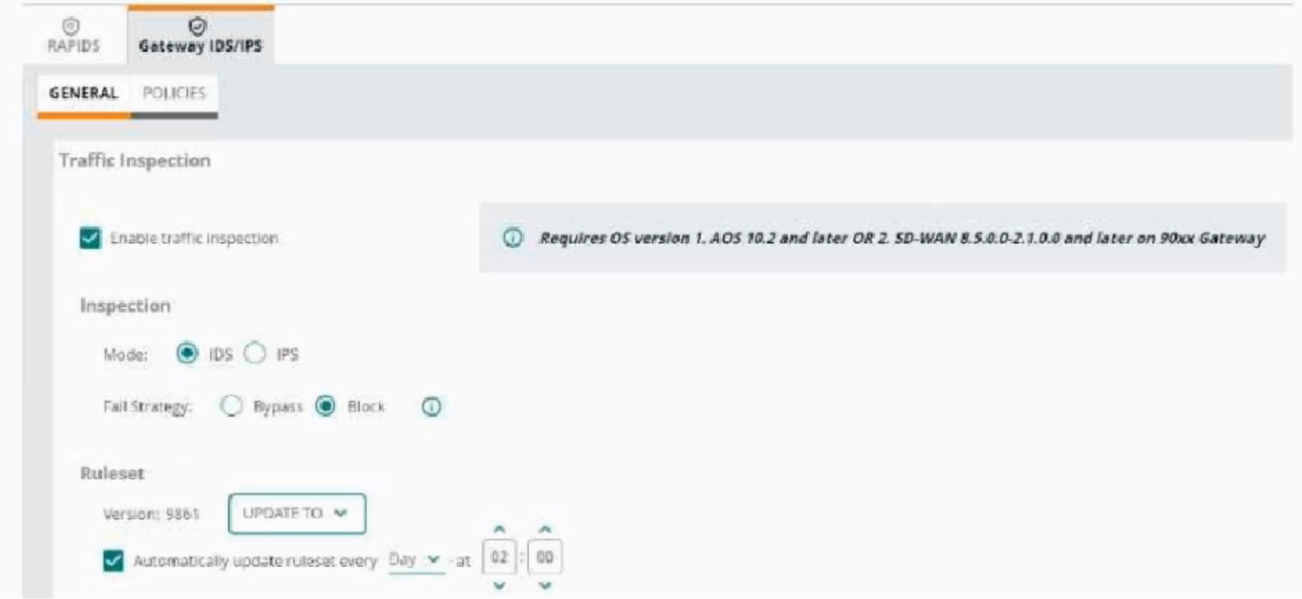
D. CPPM can submit profile information to CPDI, but if CPDI derives a different classification, CPDI takes precedence.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #18 Topic 1

Refer to the exhibit.



Traffic Inspection

☑ Enable traffic inspection

ⓘ ***Requires OS version 1. AOS 10.2 and later OR 2. SD-WAN 8.5.0.0-2.1.0.0 and later on 90xx Gateway***

Inspection

Mode: ● IDS ○ IPS

Fail Strategy: ○ Bypass ● Block ⓘ

Ruleset

Version: 9861 UPDATE TO

☑ Automatically update ruleset every Day at 02 : 00

(Note that the HPE Aruba Networking Central interface shown here might look slightly different from what you see in your HPE Aruba Networking Central interface as versions change; however, similar concepts continue to apply.)

An HPE Aruba Networking 9x00 gateway is part of an HPE Aruba Networking Central group that has the settings shown in the exhibit. What would cause the gateway to drop traffic as part of its IDPS settings?

A. Its site-to-site VPN connections failing

B. Traffic matching a rule in the active ruleset

C. Its IDPS engine failing

D. Traffic showing anomalous behavior

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

You are establishing a cluster of HPE Aruba Networking ClearPass servers. (Assume that they are running version 6.9).
For which type of certificate it is recommended to install a CA-signed certificate on the Subscriber before it joins the cluster?

A. HTTPS

B. Database

C. RADIUS/EAP

D. RadSec

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

A company has HPE Aruba Networking gateways that implement gateway IDS/IPS. Admins sometimes check the Security Dashboard, but they want a faster way to discover if a gateway starts detecting threats in traffic.
What should they do?

A. Set up Webhooks that are attached to the HPE Aruba Networking Central Threat Dashboard.

B. Use Syslog to integrate the gateways with HPE Aruba Networking ClearPass Policy manager (CPPM) event processing.

C. Set up email notifications using HPE Aruba Networking Central's global alert settings.

D. Integrate HPE Aruba Networking ClearPass Device Insight (CPDI) with Central and schedule hourly reports.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

A company has Aruba APs that are controlled by Central and that implement WIDS. When you check WIDS events, you see a “detect valid SSID misuse” event. What can you interpret from this event, and what steps should you take?

A. Clients are failing to authenticate to corporate SSIDs. You should first check for misconfigured authentication settings and then investigate a possible threat.

B. Admins have likely misconfigured SSID security settings on some of the company’s APs. You should have them check those settings.

C. Hackers are likely trying a pose as authorized APs. You should use the detecting radio information and immediately track down the device that triggered the event.

D. This event might be a threat but is almost always a false positive. You should wait to see the event over several days before following up on it.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

As part of setting up an HPE Aruba Networking ClearPass Onboard solution for wireless clients, you created Network Settings, a Configuration Profile, and a Provisioning Settings on ClearPass Onboard. You also ran the ClearPass Onboard Service Only Template on ClearPass Policy Manager (CPPM). You need to ensure that only domain users are authenticated and allowed to log into the ClearPass Onboard portal.
Which component should you edit?

A. The 802.1X services on CPPM for wireless clients

B. The ClearPass Onboard Service Pre-Auth service on CPPM

C. The Provisioning profile on ClearPass Onboard

D. The Network Settings on ClearPass Onboard

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

A company is using HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application). In the CPDI security settings, Security Analysis is On, the Data Source is ClearPass Devices Insight, and Enable Posture Assessment is On. You see that device has a Risk Score of 90. What can you know from this information?

A. The posture is unknown, and CPDI has detected exactly four vulnerabilities on the device.

B. The posture is healthy, but CPDI has detected multiple vulnerabilities on the device.

C. The posture is unhealthy, and CPDI has also detected at least one vulnerability on the device.

D. The posture is unhealthy, but CPDI has not detected any vulnerabilities on the device.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #24

Topic 1

A company has HPE Aruba Networking APs and AOS-CX switches. The APs bridge wireless traffic. They receive DHCP IP addresses on VLAN 18. Wireless users are assigned to VLAN 12. The company wants APIs to start using 802.1X authentication.
You are configuring the port-access role to which the APs are assigned post-authentication.
What is one recommended setting for that role?

A. Trust for DSCP

B. Access VLAN 18 with no support for VLAN 12

C. Auth-mode left at client-mode

D. No trust for DSCP

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Which statement describes Zero Trust Security?

A. Companies must apply the same access controls to all users, regardless of identity.

B. Companies that support remote workers cannot achieve zero trust security and must determine if the benefits outweigh the cost.

C. Companies should focus on protecting their resources rather than on protecting the boundaries of their internal network.

D. Companies can achieve zero trust security by strengthening perimeter security to detect a wider range of threats.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

A company is using HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application). You have identified a device, which is currently classified as one type, but you want to classify it as a custom type. You also want to classify all devices with similar attributes as this type, both already-discovered devices and new devices discovered later.

What should you do?

A. Create a user tag from the Generic Devices page, select the desired attributes for the tag, and save the tag.

B. In the device details, select filter, create a user tag based on the device attributes, and save the tag.

C. In the device details, select reclassify, create a user rule based on its attributes, and choose “Save & Reclassify.”

D. Create a user rule from the Generic Devices page, select the desired attributes for the rule, and choose “Save.”

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

A company has AOS-CX switches. The company wants to make is simpler and faster to admins to detect denial of service (DoS) attacks, such as ping or ARP floods, launched against the switches.
What can you do to support this use case?

A. Deploy an NAE agent on the switches to monitor control plane policing (CoPP).

B. Configure the switches to implement RADIUS accounting to HPE Aruba Networking ClearPass and enable HPE Aruba Networking ClearPass Insight.

C. Implement ARP inspection on all VLANs that support end-user devices.

D. Enabling debugging of security functions on the switches.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

A company has AOS-CX switches at the access layer, these switches are managed by the HPE Aruba Networking Central. You have identified suspicious activity on a wired client. You want to analyze the client's traffic with Wireshark, which you have on your management station.
What should you do?

A. Access the client's switch's CLI from your management station. Access the switch shell and run a TCP dump on the client port.

B. Go to the client's switch in HPE Aruba Networking Central. Use the "Security" page to run a packet capture.

C. Set up a policy that implements a captive portal redirect to your management station. Apply that policy to the client's port.

D. Set up a mirror session on the client's switch; set the client port as the source and your station IP address as the tunnel destination.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #29

Topic 1

What is a use case for running periodic subnet scans on devices from HPE Aruba Networking ClearPass Policy Manager (CPPM)?

A. Detecting devices that fail to comply with rules defined in CPPM posture policies.

B. Identifying issues with authenticating and authorizing clients

C. Using WMI to collect additional information about Windows domain clients

D. Using DHCP fingerprints to determine a client’s device category and OS

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #30 Topic 1

HPE Aruba Networking Central displays a Gateway Threat Count alert in the alert list. How can you gather more information about what caused the alert to trigger?

A. Use HPE Aruba Networking Central tools to run a Network Check on the gateway with which the alert is associated.

B. Use Live Monitoring on the gateway to download a packet capture of recent traffic flowing through the gateway.

C. Check the threat list for the gateway associated with the alert. Access threat details and download packet info.

D. Check the gateway's Audit Trail in HPE Aruba Networking Central for more details about the threats that triggered the alert.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

You are proposing HPE Aruba Networking ZTNA to an organization, which is currently using a third-party, IPsec-based client-to-site VPN. What is one advantage of ZTNA that you should emphasize?

A. ZTNA improves security for SaaS applications, which now makes up the majority of remote user traffic.

B. ZTNA shrinks the attack surface, eliminating publicly exposed ports and reducing the extent of the private network exposed to remote users.

C. ZTNA is specifically designed to enhance security for Internet of Things (IoT) devices, which are proliferating rapidly and which traditional client-to-site VPNs cannot address.

D. ZTNA offers no greater security than the current solution, but it makes it much easier for admins to create and maintain consistent policies.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

A company wants HPE Aruba Networking ClearPass Policy Manager (CPPM) to periodically poll Microsoft Endpoint Manager (formerly Intune) for attributes about its managed clients.
What should you do on ClearPass to permit this integration?

A. Install the Intune extension from ClearPass Guest.

B. Configure Endpoint Manager (Intune) as an event source on CPPM.

C. Import the Intune dictionary to the ClearPass dictionaries.

D. Create an Intune authentication source on CPPM.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

What is one use case that companies can fulfill using HPE Aruba Networking ClearPass Policy Manager’s (CPPM’s) Device Profiler?

A. Authenticating clients to Active Directory computer accounts

B. Identifying OS, browser, and application vulnerabilities by CVE ID

C. Applying the correct enforcement profiles to specialized clients as security cameras

D. Quarantining and remediating devices that have disabled firewalls

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

A company has HPE Aruba Networking Central-managed APs. The company wants to block all clients connected through the APs from using YouTube.

Which steps should you take?

A. Enable WebCC on all client firewall roles. Then, create WebCC category rules that deny suspicious URLs.

B. Enable DPI. Then, create application rules to deny YouTube on the firewall roles.

C. Enable Client IPS at the “custom” level, and then specify the check for YouTube.

D. Deploy gateways and have the APIs tunnel traffic to the gateways. Then, enable the gateway IDS/IPS engine.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

A company wants to use the HPE Aruba Networking ClearPass OnGuard agent to assign posture to clients.
How do you define the conditions by which a client receives a particular posture?

A. Create rules directly in a service's Posture tab.

B. Create rules within a WebAuth enforcement policy.

C. Create the rules directly in a service's Enforcement tab.

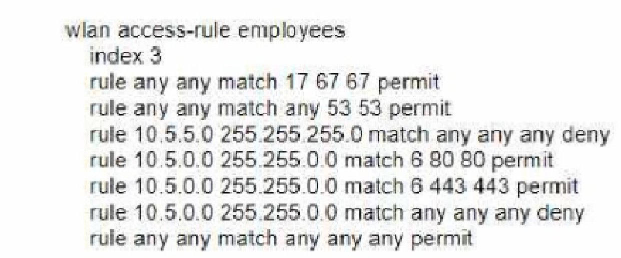
D. Create rules within a posture policy.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

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. HTTPS traffic from 10.2.2.2 to 10.5.5.5 is denied.

B. HTTPS traffic from 10.2.2.2 to 203.0.113.12 is denied.

C. Traffic from 10.5.3.3 in an active HTTPS session between 10.2.2.2 and 10.5.3.3 is permitted.

D. Traffic from 198.51.100.12 in an active HTTP session between 10.2.2.2 and 198.51.100.12 is denied.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

You need to set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to provide certificate-based authentication of 802.1X supplicants. How should you upload the root CA certificate for the supplicants' certificates?

A. As a ClearPass Server certificate with the RADIUS/EAP usage

B. As a ClearPass Server certificate with the Database usage

C. As a Trusted CA with the AD/LDAP usage

D. As a Trusted CA with the EAP usage

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

You are setting up policy rules in HPE Aruba Networking SSE. You want to create a single rule that permits users in a particular user group to access multiple applications. What is an easy way to meet this need?

A. Associate the applications directly with the IdP used to authenticate the users; chose any for the destination in the policy rule

B. Apply the same tag to the applications; select the tag as a destination in the policy rule

C. Place all the applications in the same connector zone; select that zone as a destination in the policy rule

D. Select the applications within a non-default web profile, select that profile in the policy rule

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #39

Topic 1

A company has a variety of HPE Aruba Networking solutions, including an HPE Aruba Networking infrastructure and HPE Aruba Networking ClearPass Policy Manager (CPPM). The company passes traffic from the corporate LAN destined to the data center through a third-party SRX firewall. The company would like to further protect itself from internal threats.
What is one solution that you can recommend?

A. Have the third-party firewall send Syslogs to CPPM, which can work with network devices to lock internal attackers out of the network.

B. Add ClearPass Device Insight (CPDI) to the solution, integrate it with the third-party firewall to develop more complete device profiles.

C. Configure CPPM to poll the third-party firewall for a broad array of information about internal clients, such as profile and posture.

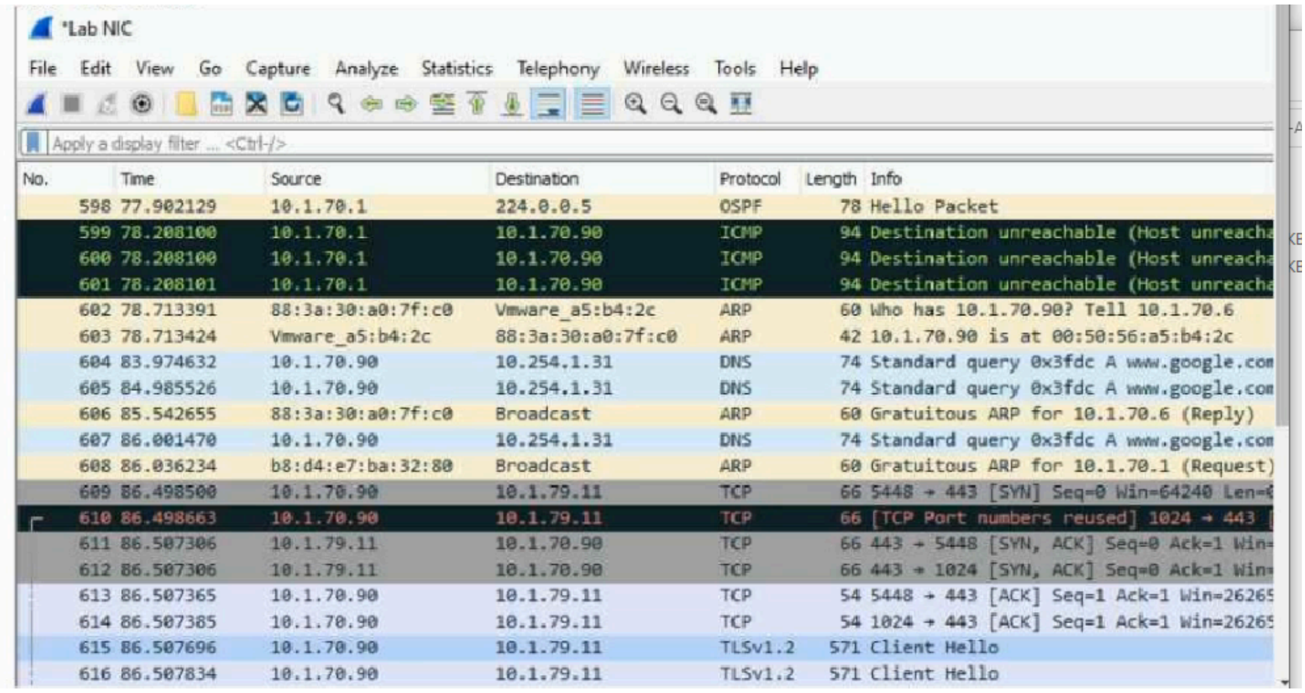
D. Use tunnel mode SSIDs and user-based tunneling (UBT) on AOS-CX switches to pass all internal traffic directly through the third-party firewall.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Refer to the exhibit.


*Lab NIC
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source             Destination        Protocol Length Info
  598 77.902129  10.1.70.1          224.0.0.5          OSPF       78 Hello Packet
  599 78.208100  10.1.70.1          10.1.70.90         ICMP       94 Destination unreachable (Host unreacha
  600 78.208100  10.1.70.1          10.1.70.90         ICMP       94 Destination unreachable (Host unreacha
  601 78.208101  10.1.70.1          10.1.70.90         ICMP       94 Destination unreachable (Host unreacha
  602 78.713391  88:3a:30:a0:7f:c0  Vmware_a5:b4:2c    ARP        60 Who has 10.1.70.90? Tell 10.1.70.6
  603 78.713424  Vmware_a5:b4:2c    88:3a:30:a0:7f:c0  ARP        42 10.1.70.90 is at 00:50:56:a5:b4:2c
  604 83.974632  10.1.70.90         10.254.1.31        DNS        74 Standard query 0x3fdc A www.google.com
  605 84.985526  10.1.70.90         10.254.1.31        DNS        74 Standard query 0x3fdc A www.google.com
  606 85.542655  88:3a:30:a0:7f:c0  Broadcast          ARP        60 Gratuitous ARP for 10.1.70.6 (Reply)
  607 86.001470  10.1.70.90         10.254.1.31        DNS        74 Standard query 0x3fdc A www.google.com
  608 86.036234  b8:d4:e7:ba:32:80  Broadcast          ARP        60 Gratuitous ARP for 10.1.70.1 (Request)
  609 86.498500  10.1.70.90         10.1.79.11         TCP        66 5448 → 443 [SYN] Seq=0 Win=64240 Len=
  610 86.498663  10.1.70.90         10.1.79.11         TCP        66 [TCP Port numbers reused] 1024 → 443 [
  611 86.507306  10.1.79.11         10.1.70.90         TCP        66 443 → 5448 [SYN, ACK] Seq=0 Ack=1 Win=
  612 86.507306  10.1.79.11         10.1.70.90         TCP        66 443 → 1024 [SYN, ACK] Seq=0 Ack=1 Win=
  613 86.507365  10.1.70.90         10.1.79.11         TCP        54 5448 → 443 [ACK] Seq=1 Ack=1 Win=2626
  614 86.507385  10.1.70.90         10.1.79.11         TCP        54 1024 → 443 [ACK] Seq=1 Ack=1 Win=2626
  615 86.507696  10.1.70.90         10.1.79.11         TLSv1.2   571 Client Hello
  616 86.507834  10.1.70.90         10.1.79.11         TLSv1.2   571 Client Hello
```

The exhibit shows a saved packet capture, which you have opened in Wireshark. You want to focus on the complete conversation between 10.1.70.90 and 10.1.79.11 that uses source port 5448.

What is a simple way to do this in Wireshark?

A. Apply a capture filter that selects for both the 10.1.70.90 and 10.1.79.11 IP addresses.

B. Click the Source column and then the Destination column to sort the packets into the desired order.

C. Apply a capture filter that selects for TCP port 5448.

D. Right-click one of the packets between those addresses and choose to follow the stream.

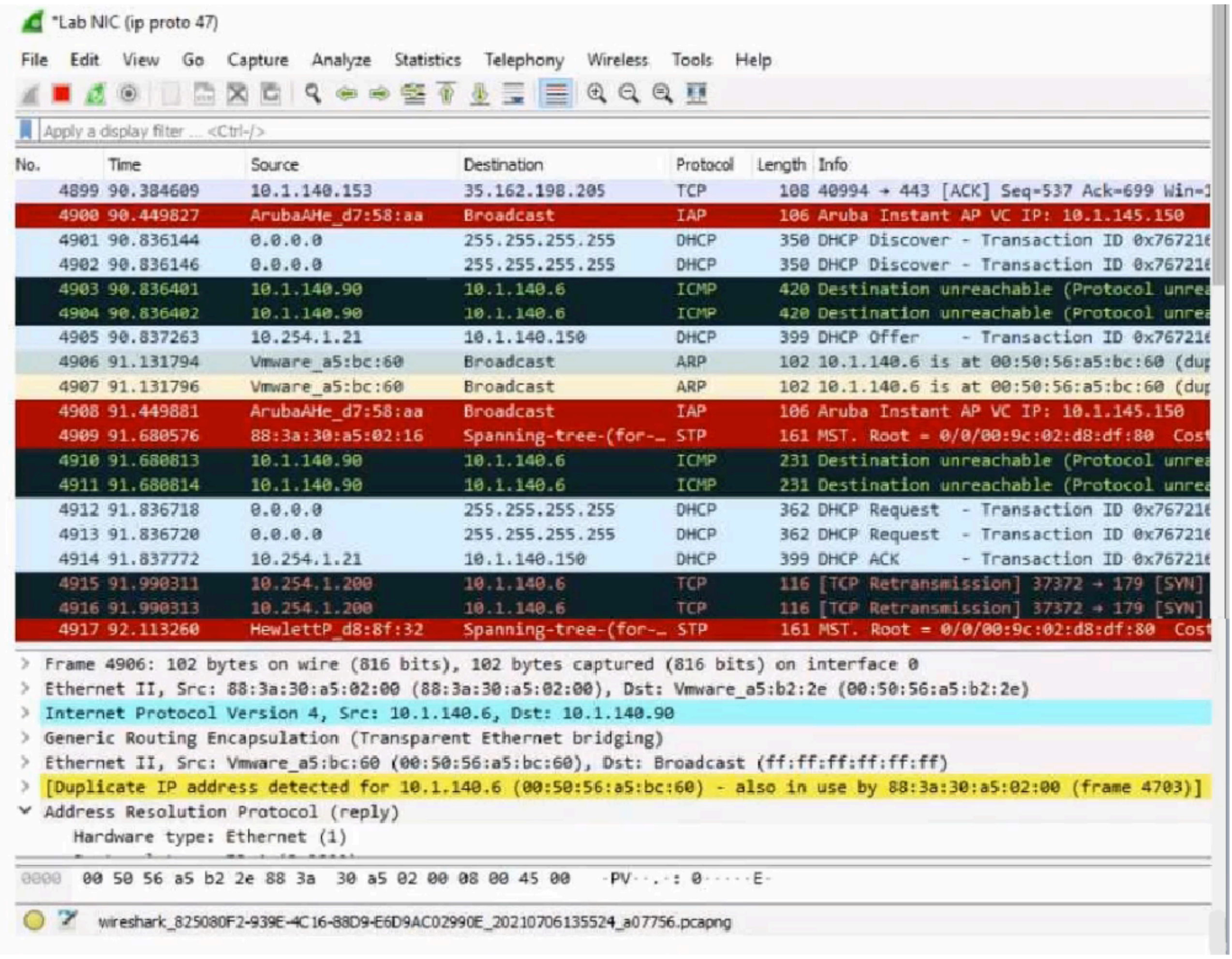
Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #41

Topic 1

Refer to the exhibit.



```
No.       Time       Source              Destination          Protocol  Length Info
     4899 90.384609  10.1.140.153        35.162.198.205       TCP       108 40994 → 443 [ACK] Seq=537 Ack=699 Win=1
     4900 90.449827  ArubaAHe_d7:58:aa   Broadcast            IAP       106 Aruba Instant AP VC IP: 10.1.145.150
     4901 90.836144  0.0.0.0             255.255.255.255      DHCP      350 DHCP Discover - Transaction ID 0x767216
     4902 90.836146  0.0.0.0             255.255.255.255      DHCP      350 DHCP Discover - Transaction ID 0x767216
     4903 90.836401  10.1.140.90         10.1.140.6           ICMP      420 Destination unreachable (Protocol unrea
     4904 90.836402  10.1.140.90         10.1.140.6           ICMP      420 Destination unreachable (Protocol unrea
     4905 90.837263  10.254.1.21         10.1.140.150         DHCP      399 DHCP Offer    - Transaction ID 0x767216
     4906 91.131794  Vmware_a5:bc:60     Broadcast            ARP       102 10.1.140.6 is at 00:50:56:a5:bc:60 (dup
     4907 91.131796  Vmware_a5:bc:60     Broadcast            ARP       102 10.1.140.6 is at 00:50:56:a5:bc:60 (dup
     4908 91.449881  ArubaAHe_d7:58:aa   Broadcast            IAP       106 Aruba Instant AP VC IP: 10.1.145.150
     4909 91.680576  88:3a:30:a5:02:16   Spanning-tree-(for-… STP       161 MST. Root = 0/0/00:9c:02:d8:df:80  Cost
     4910 91.680813  10.1.140.90         10.1.140.6           ICMP      231 Destination unreachable (Protocol unrea
     4911 91.680814  10.1.140.90         10.1.140.6           ICMP      231 Destination unreachable (Protocol unrea
     4912 91.836718  0.0.0.0             255.255.255.255      DHCP      362 DHCP Request  - Transaction ID 0x767216
     4913 91.836720  0.0.0.0             255.255.255.255      DHCP      362 DHCP Request  - Transaction ID 0x767216
     4914 91.837772  10.254.1.21         10.1.140.150         DHCP      399 DHCP ACK      - Transaction ID 0x767216
     4915 91.990311  10.254.1.200        10.1.140.6           TCP       116 [TCP Retransmission] 37372 → 179 [SYN]
     4916 91.990313  10.254.1.200        10.1.140.6           TCP       116 [TCP Retransmission] 37372 → 179 [SYN]
     4917 92.113260  HewlettP_d8:8f:32   Spanning-tree-(for-… STP       161 MST. Root = 0/0/00:9c:02:d8:df:80  Cost

> Frame 4906: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: 88:3a:30:a5:02:00 (88:3a:30:a5:02:00), Dst: Vmware_a5:b2:2e (00:50:56:a5:b2:2e)
> Internet Protocol Version 4, Src: 10.1.140.6, Dst: 10.1.140.90
> Generic Routing Encapsulation (Transparent Ethernet bridging)
> Ethernet II, Src: Vmware_a5:bc:60 (00:50:56:a5:bc:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> [Duplicate IP address detected for 10.1.140.6 (00:50:56:a5:bc:60) - also in use by 88:3a:30:a5:02:00 (frame 4703)]
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)

0000  00 50 56 a5 b2 2e 88 3a  30 a5 02 00 08 00 45 00   ·PV··.·: 0·····E·

wireshark_825080F2-939E-4C16-88D9-E6D9AC02990E_20210706135524_a07756.pcapng
```

These packets have been captured from VLAN 10, which supports clients that receive their IP addresses with DHCP.

What can you interpret from the packets that you see here?

A. Someone is possibly implementing a MAC spoofing attack to again unauthorized access.

B. The mirroring session that captured the packets was likely misconfigured and captured duplicate traffic.

C. An admin has likely misconfigured two clients to use the same DHCP settings.

D. Someone is possibly implementing an ARP poisoning and MITM attack.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

A company is using HPE Aruba Networking Central SD-WAN Orchestrator to establish a hub-spoke VPN between branch gateways (BGWs) at 1164 site and VPNCs at multiple data centers.
What is part of the configuration that admins need to complete?

A. In VPNCs' groups, establish VPN pools to control which branches connect to which VPNCs.

B. In BGWs' and VPNCs' groups, create default IKE policies for the SD-WAN Orchestrator to use.

C. In BGWs' groups, select the VPNCs to which to connect in a DC preference list.

D. At the global level, create default IPsec policies for the SD-WAN Orchestrator to use.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

A company has HPE Aruba Networking APs running AOS-10 that connect to AOS-CX switches. The APs will:
-Authenticate as 802.1X supplicants to HPE Aruba Networking ClearPass Policy Manager (CPPM)
-Be assigned to the “APs” role on the switches
-Have their traffic forwarded locally
What information do you need to help you determine the VLAN settings for the “APs” role?

A. Whether the switches are using local user-roles (LURs) or downloadable user-roles (DURs)

B. Whether the APs bridge or tunnel traffic on their SSIDs

C. Whether the switches have established tunnels with an HPE Aruba Networking gateway

D. Whether the APs have static or DHCP-assigned IP addresses

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

A company has AOS-CX switches, which authenticate clients to HPE Aruba Networking ClearPass Policy Manager (CPPM). CPPM is set up to receive a variety of information about clients' profile and posture. New information can mean that CPPM should change a client's reinforcement profile.

What should you set up on the switches to help the solution function correctly?

A. Enable RADIUS accounting to CPPM, including interim RADIUS accounting.

B. Configure a RADIUS track that references CPPM's FQDN or IP address.

C. Enable dynamic authorization, and specify CPPM as a dynamic authorization client.

D. Re-configure the authentication sever on the switch, specifying CPPM as a TACACS server.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #45 Topic 1

A company already uses HPE Aruba Networking ClearPass Policy Manager (CPPM) as the RADIUS server for authenticating wireless clients with 802.1X. Now you are setting up 802.1X on AOS-CX switches to authenticate many of those same clients on wired connections. You decide to copy CPPM's wireless 802.1X service and then edit it with a new name and enforcement policy.
What else must you change for authentication to work properly?

A. Role mapping policy

B. Authentication methods

C. Authentication source

D. Service rules

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

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 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.

B. 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.

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

D. When you plan to have CPPM issue CoAs for clients with new tags, but do not want to list those specific tags in the Device Integration settings in advance.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

You are helping an organization deploy HPE Aruba Networking SSE. What is one reason to recommend that the company install agents on remote users' devices?

A. To run posture checks and apply different permissions based on those checks

B. To permit admins to manage the HPE Aruba Networking SSE policy rules

C. To permit users to access private servers using SSH

D. To run threat inspection on clients in a local sandbox rather than in the cloud

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

You want to examine the applications that a device is using and look for any changes in application usage over several different ranges.
In which HPE Aruba Networking solution can you view this information in an easy-to-view format?

A. HPE Aruba Networking ClearPass OnGuard agent installed on the device

B. HPE Aruba Networking Central within a device's Live Monitoring page

C. HPE Aruba Networking ClearPass Insight using an Active Endpoint Security report

D. HPE Aruba Networking ClearPass Device Insight (CPDI) in the device's network activity

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

A company wants to use HPE Aruba Networking ClearPass Policy Manager (CPPM) to profile Linux devices. You have decided to schedule a subnet scan of the devices' subnets.
Which additional step should you complete before scheduling the scan?

A. Set up SSH accounts on CPPM and map them to the Linux devices' subnets.

B. Enable WMI probing in the cluster-wide parameters.

C. Enable the Data Port in the ClearPass server settings and connect that port to the network.

D. Configure SNMP in the network device settings for the switches that support the Linux devices.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

HPE Aruba Networking switches are implementing MAC-Auth to HPE Aruba Networking ClearPass Policy Manager (CPPM) for company's printers. The company wants to quarantine a client that spoofs a legitimate printer's MAC address. You plan to add a rule to the MAC-Auth service enforcement policy for this purpose.
What condition should you include?

A. Endpoint: Compliance EQUALS false

B. Endpoint: Device Insight Tag EXISTS

C. Authorization: [Endpoints Repository] Compromised EQUALS true

D. Authorization: [Endpoints Repository] Conflict EQUALS true

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

A company wants to apply role-based access control lists (ACLs) on AOS-CX switches, which are implementing authentication to HPE Aruba Networking ClearPass Policy Manager (CPPM). The company wants to centralize configuration as much as possible.
Which correctly describes your options?

A. You can configure the role on CPPM; however, the CPPM role must reference a policy name that is configured on the switch.

B. You can configure the role name on CPPM; however, the role settings, including policy and classes, must be configured locally on the switch.

C. You can configure the role, its policy, and the classes referenced in the policy all on CPPM.

D. You can configure the role and its policy on CPPM; however, the classes referenced in the policy must be configured locally on the switch.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

A company has HPE Aruba Networking APs running AOS-10 and managed by HPE Aruba Networking Central. The company also has AOS-CX switches. The security team wants you to capture traffic from a particular wireless client. You should capture this client's traffic over a 15-minute time period and then send the traffic to them in a PCAP file.

What should you do?

A. Access the CLI for the client's AP. Set up a mirroring session between its radio and a management station running Wireshark.

B. Go to the client's AP in HPE Aruba Networking Central. Use the "Security" page to run a packet capture.

C. Go to that client in HPE Aruba Networking Central. Use the "Live Events" page to run a packet capture.

D. Access the CLI for the client's AP's switch. Set up a mirroring session between the AP's port and a management station running Wireshark.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #53 *Topic 1*

A company needs you to integrate HPE Aruba Networking ClearPass Policy Manager (CPPM) with HPE Aruba Networking ClearPass Device Insight (CPDI).
What is one task you should do to prepare?

A. Install the root CA for CPPM’s HTTPS certificate as trusted in the CPDI application.

B. Enable Insight in the CPPM server configuration settings.

C. Configure WMI, SSH, and SNMP external accounts for device scanning on CPPM.

D. Collect a Data Collector token from HPE Aruba Networking Central.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #54 Topic 1

A company wants you to create a custom device fingerprint on CPPM with rules for profiling a group of specialized devices.
What is one requirement?

A. Connecting a known device of this type and getting it discovered in CPPM's Endpoints Repository

B. Enabling HPE Aruba Networking ClearPass Device Insight integration with the correct Data Collector token

C. Pre-defining the desired attributes and rules in a XML format file

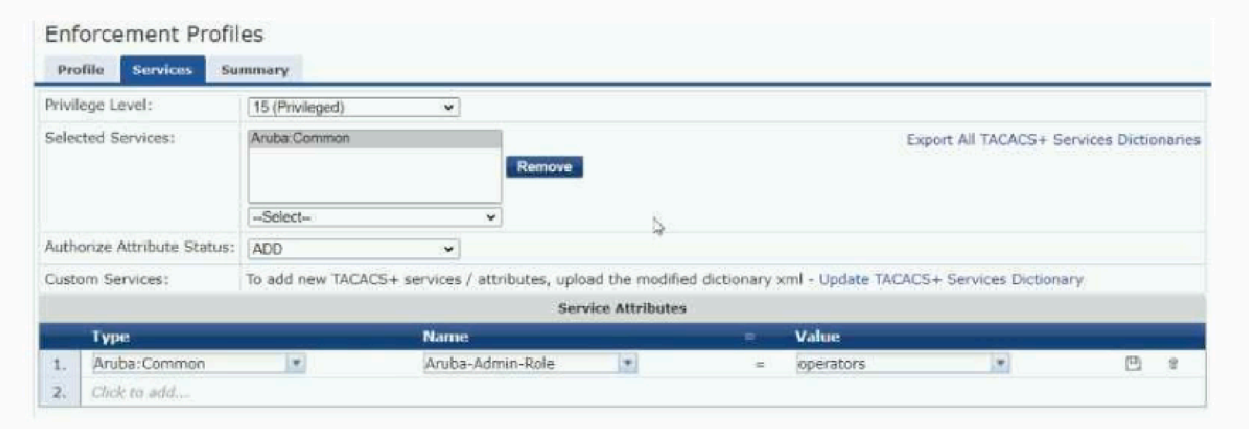
D. Disabling the Automatically download Endpoint Profiler Fingerprints feature in cluster-wide parameters.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #55 *Topic 1*

Refer to the exhibit.



Privilege Level: 15 (Privileged)

Selected Services: Aruba:Common

--Select--

Authorize Attribute Status: ADD

Custom Services: To add new TACACS+ services / attributes, upload the modified dictionary xml - Update TACACS+ Services Dictionary

Service Attributes

	Type	Name	=	Value
1.	Aruba:Common	Aruba-Admin-Role	=	operators
2.	*Click to add...*			

The exhibit shows the TACACS+ enforcement profile that HPE Aruba Networking ClearPass Policy Manager (CPPM) assigns to a manager. When this manager logs into an AOS-CX switch, what does the switch do?

A. Assigns the manager operator-level privileges

B. Assigns the manager administrator-level privileges

C. Rejects the manager with an error message

D. Assigns the manager auditor-level privileges

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

You are using Wireshark to view packets captures from HPE Aruba Networking infrastructure, but you're not sure that the packets are displaying correctly. In which circumstances does it make sense to configure Wireshark to ignore protection bits with the IV for the 802.11 protocol?

A. When the traffic was captured on the data plane of an HPE Aruba Networking gateway and sent to a remote IP

B. When the traffic was mirrored from an AOS-CX switch port connected to an AP

C. When the traffic was captured from an AP with HPE Aruba Networking Central

D. When the traffic was captured on the control plane of an HPE Aruba Networking MC and set to a remote IP

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

You have enabled “rogue AP containment” in the Wireless IPS settings for a company’s HPE Aruba Networking APs.
What form of containment does HPE Aruba Networking recommend?

A. Wireless deauthentication only

B. Wireless tarpit and wired containment

C. Wireless tarpit only

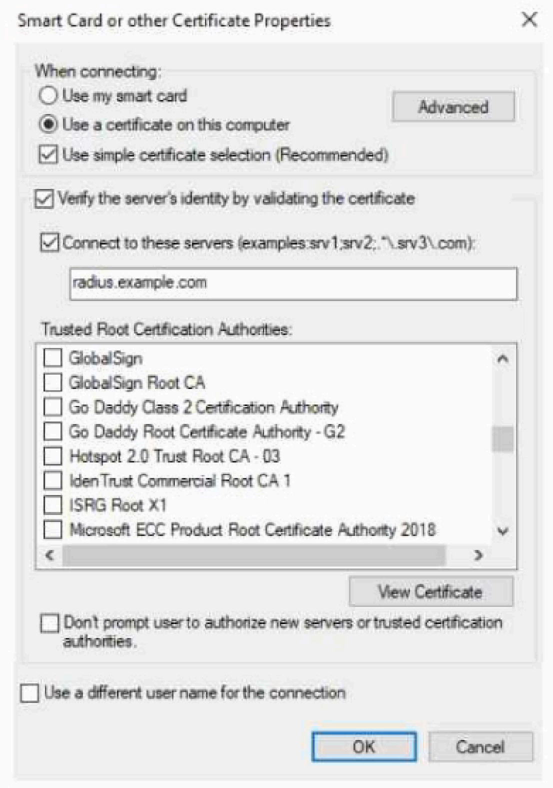
D. Wired containment

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

Refer to the exhibit.



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Verify the server's identity by validating the certificate

☑ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

radius.example.com

Trusted Root Certification Authorities:

- □ GlobalSign
- □ GlobalSign Root CA
- □ Go Daddy Class 2 Certification Authority
- □ Go Daddy Root Certificate Authority - G2
- □ Hotspot 2.0 Trust Root CA - 03
- □ IdenTrust Commercial Root CA 1
- □ ISRG Root X1
- □ Microsoft ECC Product Root Certificate Authority 2018

□ Don't prompt user to authorize new servers or trusted certification authorities.

□ Use a different user name for the connection

The exhibit shows the 802.1X-related settings for Windows domain clients.

What should admins change to make the settings follow best security practices?

A. Specify at least two server names under the “Connect to these servers” field.

B. Select the desired Trusted Root Certification Authority and select the check box next to “Don’t prompt users.”

C. Under the “Connect to these servers” field, use a wildcard in the server name.

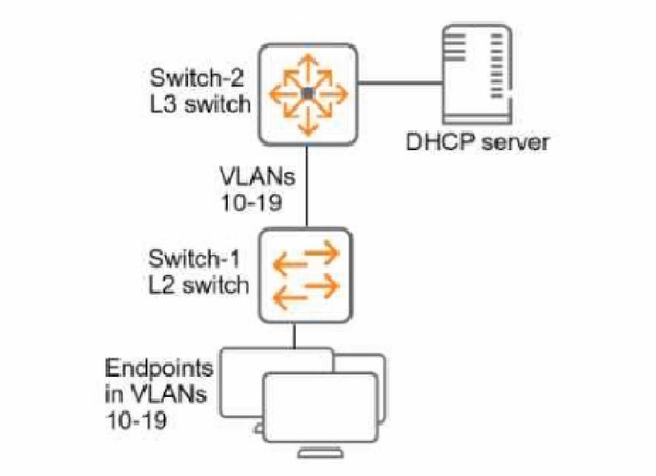
D. Clear the check box for using simple certificate selection and select the desired certificate manually.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #59 Topic 1

Refer to the exhibit.



You have verified that AOS-CX Switch-1 has constructed an IP-to-MAC binding table in VLANs 10-19. Now you need to enable ARP inspection for the endpoint connected to Switch-1.

What must you do first to prevent traffic disruption?

A. Configure ARP inspection on VLANs 10-19 on Switch-2.

B. Configure DHCP snooping on VLANs 10-19 on Switch-2.

C. Configure Switch-1 uplinks as trusted ARP inspection ports.

D. Create a static IP-to-MAC binding on Switch-1 for the DHCP server.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!