Free Questions for HPE6-A84 by certscare

Shared by Colon on 29-01-2024

For More Free Questions and Preparation Resources

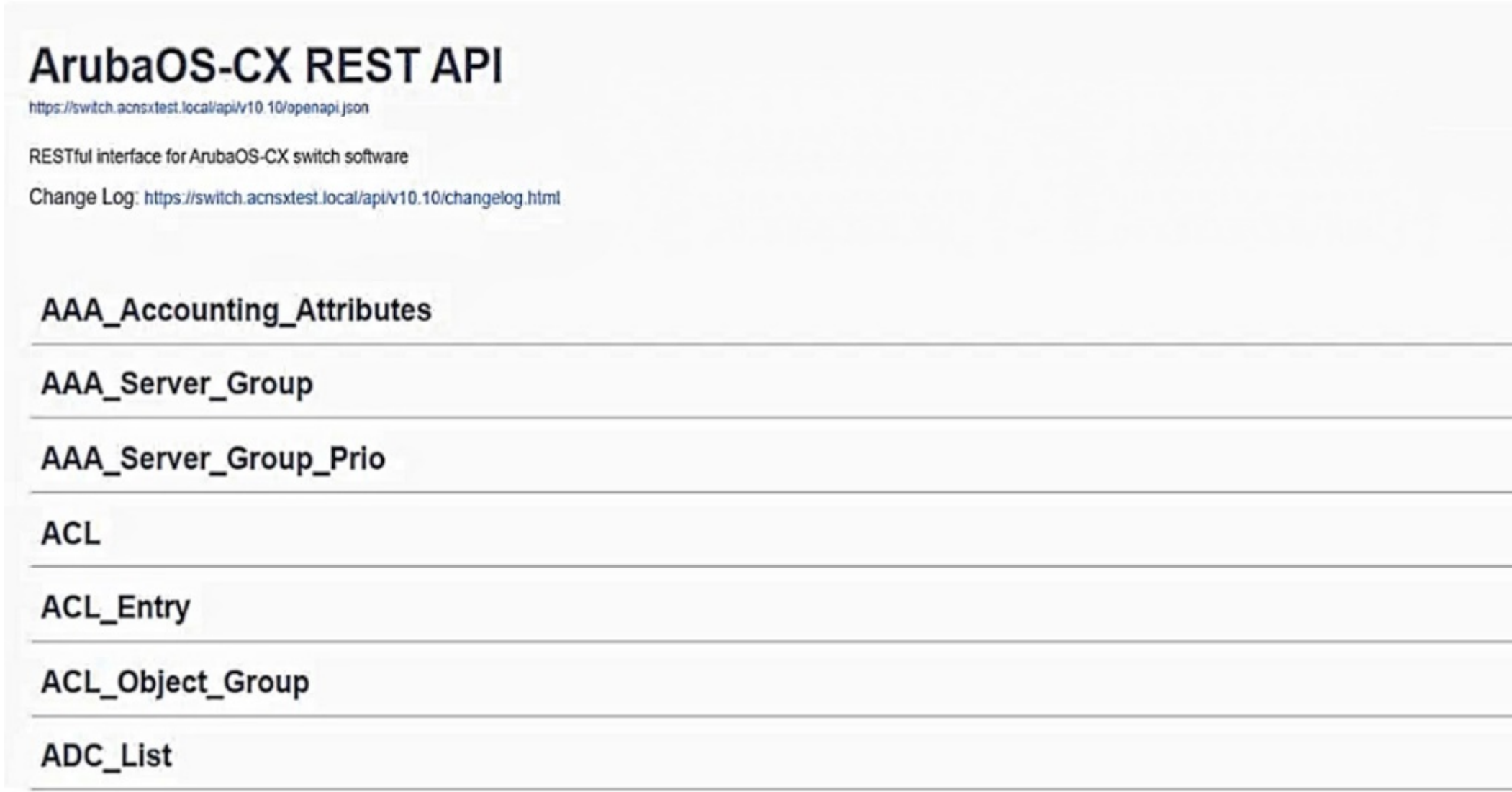
Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are working with a developer to design a custom NAE script for a customer. You are helping the developer find the correct REST API resource to monitor.

Refer to the exhibit below.



What should you do before proceeding?

Options:

A- Go to the v1 API documentation interface instead of the v10.10 interface.

B- Use your Aruba passport account and collect a token to use when trying out API calls.

C- Enable the switch to listen to REST API calls on the default VRF.

D- Make sure that your browser is set up to store authentication tokens and cookies.

Answer:

B

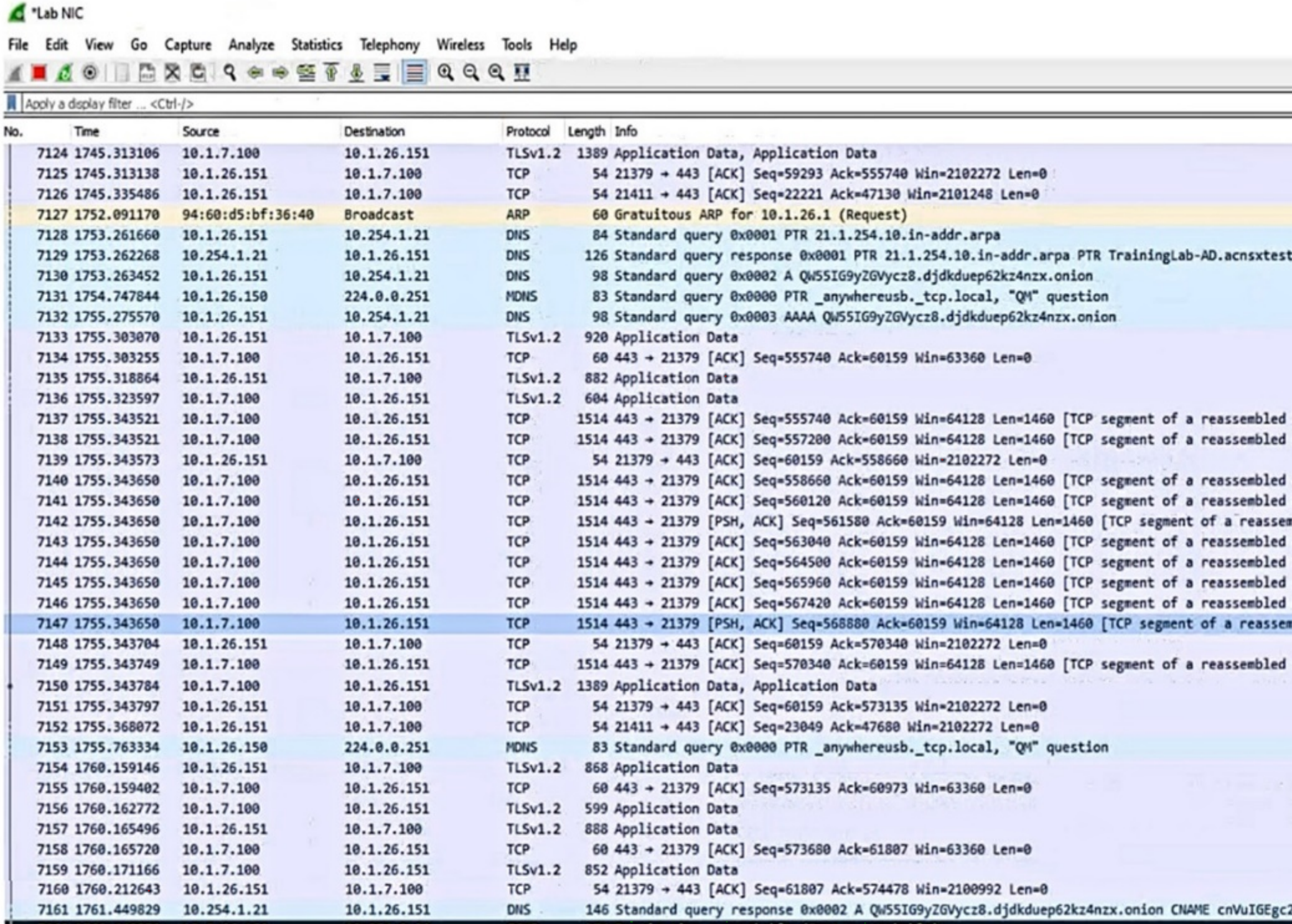
Explanation:

The exhibit shows the ArubaOS-CX REST API documentation interface, which allows you to explore the available resources and try out the API calls using the "Try it out" button. However, before you can use this feature, you need to authenticate yourself with your Aruba passport account and collect a token that will be used for subsequent requests. This token will expire after a certain time, so you need to refresh it periodically.You can find more details about how to use the documentation interface and collect a token in theArubaOS-CX REST API Guide1.

Question 2

Question Type: MultipleChoice

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
7124 1745.313106 10.1.7.100 10.1.26.151 TLSv1.2 1389 Application Data, Application Data
7125 1745.313138 10.1.26.151 10.1.7.100 TCP 54 21379 → 443 [ACK] Seq=59293 Ack=555740 Win=2102272 Len=0
7126 1745.335486 10.1.26.151 10.1.7.100 TCP 54 21411 → 443 [ACK] Seq=22221 Ack=47130 Win=2101248 Len=0
7127 1752.091170 94:60:d5:bf:36:40 Broadcast ARP 60 Gratuitous ARP for 10.1.26.1 (Request)
7128 1753.261660 10.1.26.151 10.254.1.21 DNS 84 Standard query 0x0001 PTR 21.1.254.10.in-addr.arpa
7129 1753.262268 10.254.1.21 10.1.26.151 DNS 126 Standard query response 0x0001 PTR 21.1.254.10.in-addr.arpa PTR TrainingLab-AD.acnsxtest
7130 1753.263452 10.1.26.151 10.254.1.21 DNS 98 Standard query 0x0002 A QW55IG9yZGVycz8.djdkduep62kz4nzx.onion
7131 1754.747844 10.1.26.150 224.0.0.251 MDNS 83 Standard query 0x0000 PTR _anywhereusb._tcp.local, "QM" question
7132 1755.275570 10.1.26.151 10.254.1.21 DNS 98 Standard query 0x0003 AAAA QW55IG9yZGVycz8.djdkduep62kz4nzx.onion
7133 1755.303070 10.1.26.151 10.1.7.100 TLSv1.2 920 Application Data
7134 1755.303255 10.1.7.100 10.1.26.151 TCP 60 443 → 21379 [ACK] Seq=555740 Ack=60159 Win=63360 Len=0
7135 1755.318864 10.1.26.151 10.1.7.100 TLSv1.2 882 Application Data
7136 1755.323597 10.1.7.100 10.1.26.151 TLSv1.2 604 Application Data
7137 1755.343521 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [ACK] Seq=555740 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled
7138 1755.343521 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [ACK] Seq=557200 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled
7139 1755.343573 10.1.26.151 10.1.7.100 TCP 54 21379 → 443 [ACK] Seq=60159 Ack=558660 Win=2102272 Len=0
7140 1755.343650 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [ACK] Seq=558660 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled
7141 1755.343650 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [ACK] Seq=560120 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled
7142 1755.343650 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [PSH, ACK] Seq=561580 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassem
7143 1755.343650 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [ACK] Seq=563040 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled
7144 1755.343650 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [ACK] Seq=564500 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled
7145 1755.343650 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [ACK] Seq=565960 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled
7146 1755.343650 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [ACK] Seq=567420 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled
7147 1755.343650 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [PSH, ACK] Seq=568880 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassem
7148 1755.343704 10.1.26.151 10.1.7.100 TCP 54 21379 → 443 [ACK] Seq=60159 Ack=570340 Win=2102272 Len=0
7149 1755.343749 10.1.7.100 10.1.26.151 TCP 1514 443 → 21379 [ACK] Seq=570340 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled
7150 1755.343784 10.1.7.100 10.1.26.151 TLSv1.2 1389 Application Data, Application Data
7151 1755.343797 10.1.26.151 10.1.7.100 TCP 54 21379 → 443 [ACK] Seq=60159 Ack=573135 Win=2102272 Len=0
7152 1755.368072 10.1.26.151 10.1.7.100 TCP 54 21411 → 443 [ACK] Seq=23049 Ack=47680 Win=2102272 Len=0
7153 1755.763334 10.1.26.150 224.0.0.251 MDNS 83 Standard query 0x0000 PTR _anywhereusb._tcp.local, "QM" question
7154 1760.159146 10.1.26.151 10.1.7.100 TLSv1.2 868 Application Data
7155 1760.159402 10.1.7.100 10.1.26.151 TCP 60 443 → 21379 [ACK] Seq=573135 Ack=60973 Win=63360 Len=0
7156 1760.162772 10.1.7.100 10.1.26.151 TLSv1.2 599 Application Data
7157 1760.165496 10.1.26.151 10.1.7.100 TLSv1.2 888 Application Data
7158 1760.165720 10.1.7.100 10.1.26.151 TCP 60 443 → 21379 [ACK] Seq=573680 Ack=61807 Win=63360 Len=0
7159 1760.171166 10.1.7.100 10.1.26.151 TLSv1.2 852 Application Data
7160 1760.212643 10.1.26.151 10.1.7.100 TCP 54 21379 → 443 [ACK] Seq=61807 Ack=574478 Win=2100992 Len=0
7161 1761.449829 10.254.1.21 10.1.26.151 DNS 146 Standard query response 0x0002 A QW55IG9yZGVycz8.djdkduep62kz4nzx.onion CNAME cnVuIGEgc2

Which security issue is possibly indicated by this traffic capture?

Options:

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

Answer:

C

Explanation:

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 3

Question Type: MultipleChoice

How does Aruba Central handle security for site-to-site connections between AOS 10 gateways?

Options:

A- It uses an Aruba proprietary integrity and encryption technologies to secure site-to-site connections, making them resistant to zero day attacks.

B- It automatically establishes IPsec tunnels for all site-to-site (all HUBs and Branches) connections using keys securely distributed by Central.

C- It automatically steers traffic away from Internet-based connections to more secure MPLS connections to reduce encryption overhead.

D- It automatically establishes simple-to-manage and highly secure TLSv1.3 tunnels between gateways.

Answer:

B

Explanation:

Aruba Central supports site-to-site VPNs between AOS 10 gateways, which are Aruba devices that provide routing, firewall, and VPN functions. Aruba Central can automatically provision and manage the site-to-site VPNs using the VPN Manager feature.The VPN Manager allows you to create VPN groups that consist of one or more hubs and branches, and define the VPN settings for each group1

Aruba Central uses IPsec as the protocol to secure the site-to-site connections between the AOS 10 gateways. IPsec is a standard protocol that provides encryption, authentication, and integrity for IP packets. Aruba Central automatically establishes IPsec tunnels for all site-to-site connections using keys that are securely distributed by Central. The keys are generated by Central and pushed to the gateways using a secure channel.The keys are rotated periodically to enhance security2

Question 4

Question Type: MultipleChoice

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

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

Options:

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

Answer:

A

Explanation:

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 5

Question Type: MultipleChoice

Refer to the scenario.

A customer is migrating from on-prem AD to Azure AD as its sole domain solution. The customer also manages both wired and wireless devices with Microsoft Endpoint Manager (Intune).

The customer wants to improve security for the network edge. You are helping the customer design a ClearPass deployment for this purpose. Aruba network devices will authenticate wireless and wired clients to an Aruba ClearPass Policy Manager (CPPM) cluster (which uses version 6.10).

The customer has several requirements for authentication. The clients should only pass EAP-TLS authentication if a query to Azure AD shows that they have accounts in Azure AD. To further refine the clients' privileges, ClearPass also should use information collected by Intune to make access control decisions.

You are planning to use Azure AD as the authentication source in 802.1X services.

What should you make sure that the customer understands is required?

Options:

A- An app registration on Azure AD that references the CPPM's FQDN

B- Windows 365 subscriptions

C- CPPM's RADIUS certificate was imported as trusted in the Azure AD directory

D- Azure AD Domain Services

Answer:

A

Explanation:

To use Azure AD as the authentication source in 802.1X services, you need to configure CPPM as a SAML service provider and Azure AD as a SAML identity provider. This allows CPPM to use Azure AD for user authentication and role mapping. To do this, you need to create an app registration on Azure AD that references the CPPM's FQDN as the reply URL and the entity ID.You also need to grant the app registration the required permissions to access user information from Azure AD1

Question 6

Question Type: MultipleChoice

Refer to the scenario.

A customer is migrating from on-prem AD to Azure AD as its sole domain solution. The customer also manages both wired and wireless devices with Microsoft Endpoint Manager (Intune).

The customer wants to improve security for the network edge. You are helping the customer design a ClearPass deployment for this purpose. Aruba network devices will authenticate wireless and wired clients to an Aruba ClearPass Policy Manager (CPPM) cluster (which uses version 6.10).

The customer has several requirements for authentication. The clients should only pass EAP-TLS authentication if a query to Azure AD shows that they have accounts in Azure AD. To further refine the clients' privileges, ClearPass also should use information collected by Intune to make access control decisions.

The customer wants you to configure CPPM to collect information from Intune on demand during the authentication process.

What should you tell the Intune admins about the certificates issued to clients?

Options:

A- They must be issued by a well-known, trusted CA.

B- They must include the Intune ID in the subject name.

C- They must include the client MAC address in the subject name.

D- They must be issued by a ClearPass Onboard CA.

Answer:

B

Explanation:

To configure CPPM to collect information from Intune on demand during the authentication process, you need to use the Intune extension for ClearPass. This extension allows ClearPass to query Intune for device compliance and configuration information using the Intune API.To use this extension, you need to register an app in Azure AD and grant it the required permissions to access Intune1

The Intune extension uses the device ID as the key to query Intune for device information. The device ID is a unique identifier that is assigned by Intune to each enrolled device. The device ID can be obtained from the client certificate that is used for EAP-TLS authentication.Therefore, the certificates issued to clients must include the Intune ID in the subject name, so that ClearPass can extract it and use it to query Intune2

The certificates issued to clients do not need to be issued by a well-known, trusted CA, as long as ClearPass trusts the CA that issued them. The certificates do not need to include the client MAC address in the subject name, as this is not relevant for querying Intune. The certificates do not need to be issued by a ClearPass Onboard CA, as this is not a requirement for using the Intune extension.

1: ClearPass Extensions - Microsoft Intune Integration - Aruba, section "Configuring Microsoft Extension in ClearPass"2: ClearPass Extensions - Microsoft Intune Integration - Aruba, section "Configuring EAP-TLS Authentication"