HPE6-A84 Q&As

Aruba Certified Network Security Expert Written

Pass HP HPE6-A84 Exam with 100% Guarantee

QUESTION 1

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?

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

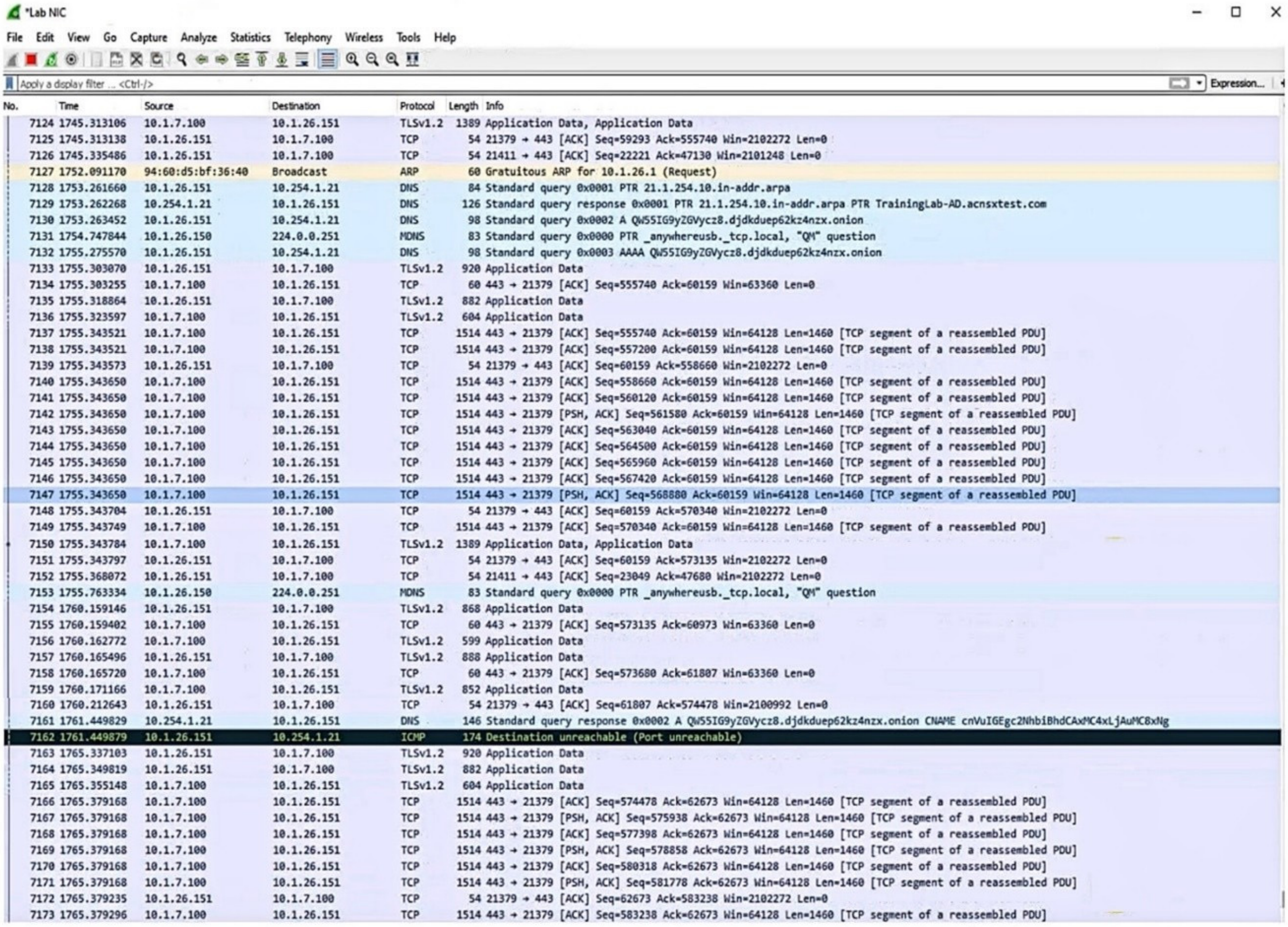
D. Azure AD Domain Services

Correct Answer: A

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 2

Refer to the exhibit.



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

```
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.com
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 PDU]
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 PDU]
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 PDU]
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 PDU]
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 reassembled PDU]
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 PDU]
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 PDU]
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 PDU]
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 PDU]
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 reassembled PDU]
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 PDU]
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 cnVuIGEgc2NhbiBhdCAxMC4xLjAuMC8xNg
7162 1761.449879  10.1.26.151        10.254.1.21   ICMP      174 Destination unreachable (Port unreachable)
7163 1765.337103  10.1.26.151        10.1.7.100    TLSv1.2   920 Application Data
7164 1765.349819  10.1.26.151        10.1.7.100    TLSv1.2   882 Application Data
7165 1765.355148  10.1.7.100         10.1.26.151   TLSv1.2   604 Application Data
7166 1765.379168  10.1.7.100         10.1.26.151   TCP      1514 443 → 21379 [ACK] Seq=574478 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7167 1765.379168  10.1.7.100         10.1.26.151   TCP      1514 443 → 21379 [PSH, ACK] Seq=575938 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7168 1765.379168  10.1.7.100         10.1.26.151   TCP      1514 443 → 21379 [ACK] Seq=577398 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7169 1765.379168  10.1.7.100         10.1.26.151   TCP      1514 443 → 21379 [PSH, ACK] Seq=578858 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7170 1765.379168  10.1.7.100         10.1.26.151   TCP      1514 443 → 21379 [ACK] Seq=580318 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7171 1765.379168  10.1.7.100         10.1.26.151   TCP      1514 443 → 21379 [PSH, ACK] Seq=581778 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7172 1765.379235  10.1.26.151        10.1.7.100    TCP        54 21379 → 443 [ACK] Seq=62673 Ack=583238 Win=2102272 Len=0
7173 1765.379296  10.1.7.100         10.1.26.151   TCP      1514 443 → 21379 [ACK] Seq=583238 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
```

Which security issue is possibly indicated by this traffic capture?

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

Correct Answer: C

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 0x2a0x2a0x2a0x2a0x2a0x2a0x2a0x2a0x2a.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

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

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

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

Correct Answer: A

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 4

Which element helps to lay the foundation for solid network security forensics?

A. Enable BPDU protection and loop protection on edqe switch ports

B. Enabling debug-level information for network infrastructure device logs

C. Implementing 802.1X authentication on switch ports that connect to APs

D. Ensuring that all network devices use a correct, consistent clock

Correct Answer: D

This is because network forensics relies on the analysis of network traffic data, which is often time-stamped by the devices that generate or transmit it. Having a synchronized and accurate clock across all network devices helps to establish a reliable timeline of events and correlate different sources of evidence12 A. Enable BPDU protection and loop protection on edge switch ports is not related to network security forensics, but rather to preventing network loops and topology changes caused by rogue switches or bridges3

B. Enabling debug-level information for network infrastructure device logs might provide more details about the network activity, but it also consumes more resources and storage, and might not be relevant or useful for forensic analysis. Moreover, debug-level information might not be available for long-term retention or legal purposes4 C. Implementing 802.1X authentication on switch ports that connect to APs is a good security practice to prevent unauthorized access to the network, but it does not directly help with network security forensics. 802.1X authentication does not capture or record network traffic data, which is the main source of evidence for network forensics

QUESTION 5

Refer to the scenario.

A customer requires these rights for clients in the "medical-mobile" AOS firewall role on Aruba Mobility Controllers (MCs):

1.

Permitted to receive IP addresses with DHCP

2.

Permitted access to DNS services from 10.8.9.7 and no other server

3.

Permitted access to all subnets in the 10.1.0.0/16 range except denied access to 10.1.12.0/22

4.

Denied access to other 10.0.0.0/8 subnets

5.

Permitted access to the Internet

6.

Denied access to the WLAN for a period of time if they send any SSH traffic

7.

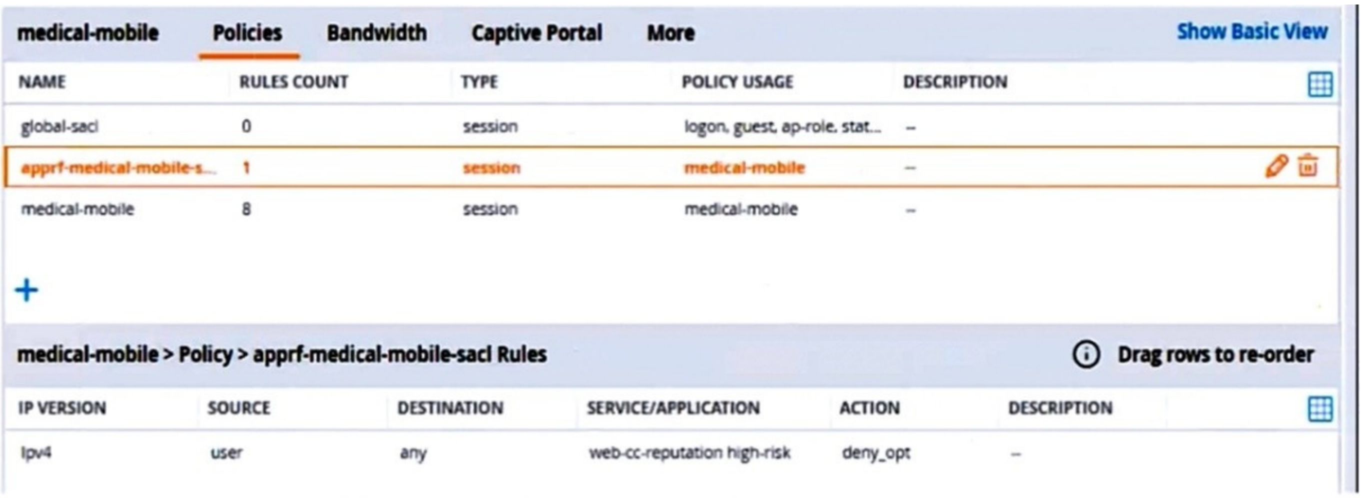
Denied access to the WLAN for a period of time if they send any Telnet traffic

8.

Denied access to all high-risk websites

External devices should not be permitted to initiate sessions with "medical-mobile" clients, only send return traffic.

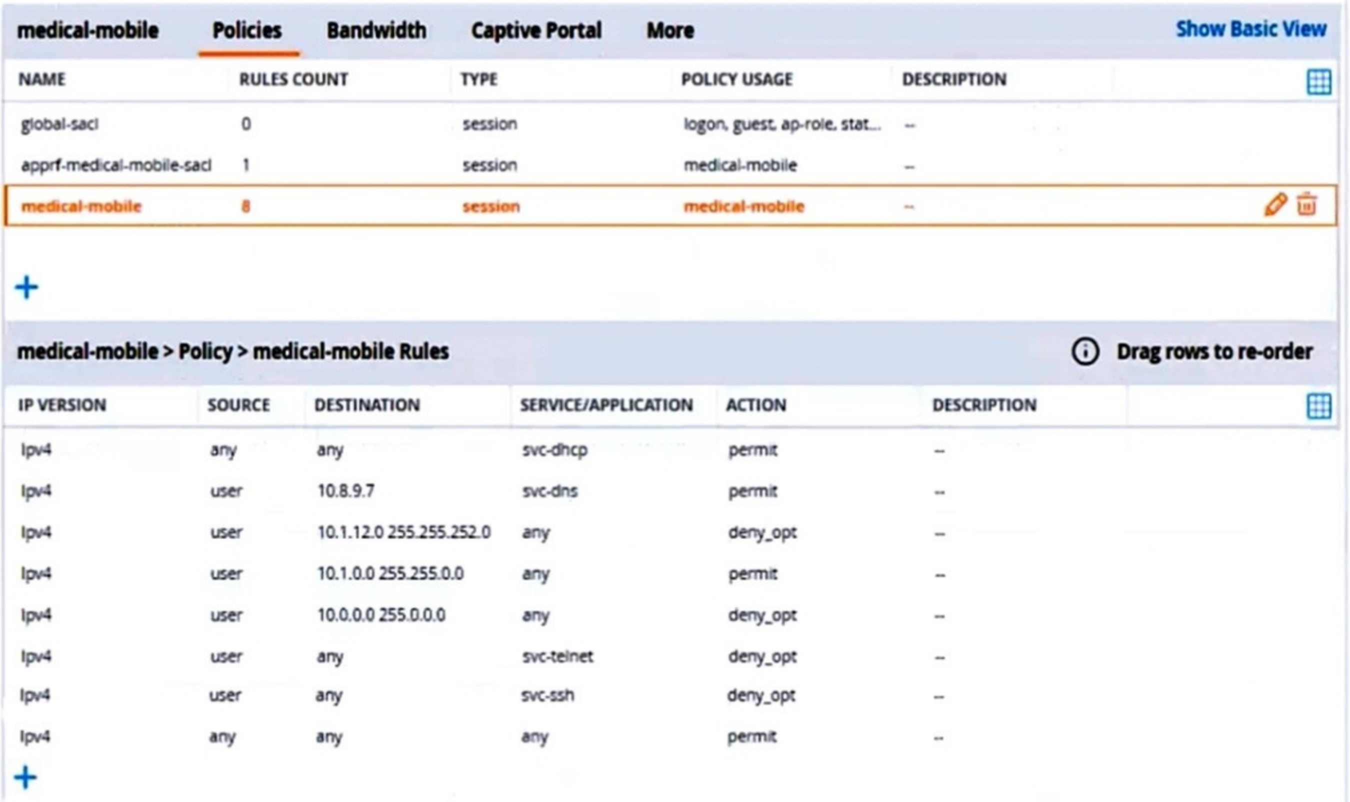
The exhibits below show the configuration for the role.



NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	–
apprf-medical-mobile-s...	1	session	medical-mobile	–
medical-mobile	8	session	medical-mobile	–

medical-mobile > Policy > apprf-medical-mobile-sacl Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
Ipv4	user	any	web-cc-reputation high-risk	deny_opt	–



NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	–
apprf-medical-mobile-sacl	1	session	medical-mobile	–
medical-mobile	8	session	medical-mobile	–

medical-mobile > Policy > medical-mobile Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
Ipv4	any	any	svc-dhcp	permit	–
Ipv4	user	10.8.9.7	svc-dns	permit	–
Ipv4	user	10.1.12.0 255.255.252.0	any	deny_opt	–
Ipv4	user	10.1.0.0 255.255.0.0	any	permit	–
Ipv4	user	10.0.0.0 255.0.0.0	any	deny_opt	–
Ipv4	user	any	svc-telnet	deny_opt	–
Ipv4	user	any	svc-ssh	deny_opt	–
Ipv4	any	any	any	permit	–

There are multiple issues with the configuration.

What is one of the changes that you must make to the policies to meet the scenario requirements? (In the options, rules in a policy are referenced from top to bottom. For example, "medical-mobile" rule 1 is "ipv4 any any svc-dhcp permit," and rule 8 is "ipv4 any any any permit\\'.)

A. In the "medical-mobile" policy, change the source in rule 1 to "user."

B. In the "medical-mobile" policy, change the subnet mask in rule 3 to 255.255.248.0.

C. In the "medical-mobile" policy, move rules 6 and 7 to the top of the list.

D. Move the rule in the "apprf-medical-mobile-sacl" policy between rules 7 and 8 in the "medical-mobile" policy.

Correct Answer: C

Rules 6 and 7 in the "medical-mobile" policy are used to deny access to the WLAN for a period of time if the clients send any SSH or Telnet traffic, as required by the scenario. However, these rules are currently placed below rule 5, which permits access to the Internet for any traffic. This means that rule 5 will override rules 6 and 7, and the clients will not be denied access to the WLAN even if they send SSH or Telnet traffic. To fix this issue, rules 6 and 7 should be moved to the top of the list, before rule 5. This way, rules 6 and 7 will take precedence over rule 5, and the clients will be denied access to the WLAN if they send SSH or Telnet traffic, as expected.