

[Sep-2020] Valid NSE7_SAC-6.2 Exam Dumps PDF Free Download in Braindump2go [Q15-Q26]

2020/September Latest Braindump2go NSE7_SAC-6.2 Exam Dumps with PDF and VCE Free Updated Today! Following are some new NSE7_SAC-6.2 Real Exam Questions!

QUESTION 15 What does DHCP snooping MAC verification do?

A. Drops DHCP release packets on untrusted ports.

B. Drops DHCP packets with no relay agent information (option 82) on untrusted ports.

C. Drops DHCP offer packets on untrusted ports.

D. Drops DHCP packets on untrusted ports when the client hardware address does not match the source MAC address.

Answer: C

QUESTION 16 Which statement correctly describes the guest portal behavior on FortiAuthenticator?

A. Sponsored accounts cannot authenticate using guest portals.

B. FortiAuthenticator uses POST parameters and a RADIUS client configuration to map the request to a guest portal for authentication.

C. All guest accounts must be activated using SMS or email activation codes.

D. All self-registered and sponsored accounts are listed on the local Users GUI page on FortiAuthenticator.

Answer: A

QUESTION 17 Examine the sections of the configuration shown in the following output;

```
config vpn cert
    set ocap-st
    set ocap-de
    set strict-
end
config vpn cert
    set uri
    set uns
next
end
config vpn ssl
    set ssl-ocsp
end
```

What action will the FortiGate take when using OCSP certificate validation?

A. FortiGate will reject the certificate if the OCSP server replies that the certificate is unknown.

B. FortiGate will use the OCSP server 10.0.1.150 even when the OCSP URL field in the user certificate contains a different OCSP server IP address.

C. FortiGate will use the OCSP server 10.0.1.150 even when there is a different OCSP IP address in the ocap-override-server option under config user peer.

D. FortiGate will invalidate the certificate if the OCSP server is unavailable.

Answer: C

QUESTION 18 Refer to the exhibit.

```
FortiGate # diagnose test authserver ldap training-lab student password
(2160) handle_req-Recv auth req 1504903d16 for student in Training-Lab opt=0000001b prot=0
(260) _compert_group_list_from_req-group 'Training-Lab'
(406) fthand_pop3_start-student
(1038) _fthand_cfg_get_ldap_list_by_server-loading LDAP server 'Training-Lab'
(1544) fthand_ldap_init-search filter is: sAMAccountName=student
(1552) fthand_ldap_init-search base is: cn=users,dc=trainingad,dc=training,dc=lab
(973) _fthand_ldap_dns_cb-Resolved Training-Lab (idx 0) to 10.0.1.10
(1021) _fthand_ldap_dns_cb-still connecting.
(817) create_auth_session-Total 1 server(s) to try
(909) _ldap_connect-rcpa connect(10.0.1.10) is established.
(814) _ldap_extn-state 3 (Admin Binding)
(194) _ldap_build_bind_req-Binding to 'CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab'
(802) fthand_ldap_send-sending 80 bytes to 10.0.1.10
(845) fthand_ldap_send-request is sent. ID 1
(814) _ldap_extn-state 4 (Admin Bind resp)
(1056) fthand_ldap_recv-Response len: 14, svr: 10.0.1.10
(754) fthand_ldap_parse_response-Got one MESSAGE. ID1, type:bind
(814) _ldap_extn-state 5 (User Binding)
(854) fthand_ldap_build_dn-search req-base 'cn=users,dc=trainingad,dc=training,dc=lab' filter:sAMAccountName=student
(852) fthand_ldap_send-sending 99 bytes to 10.0.1.10
(844) fthand_ldap_send-request is sent. ID 2
(814) _ldap_extn-state 12 (DN search resp)
(1056) fthand_ldap_recv-Response len: 69, svr: 10.0.1.10
(754) fthand_ldap_parse_response-Got one MESSAGE. ID12, type:search-entry
(791) fthand_ldap_parse_response-ret=0
(1059) _fthand_ldap_dn_entry-Get DN 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
(90) ldap dn list add-added CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab
(1056) fthand_ldap_recv-Response len: 14, svr: 10.0.1.10
(754) fthand_ldap_parse_response-Got one MESSAGE. ID12, type:search-result
(791) fthand_ldap_parse_response-ret=0
(801) _ldap_extn-change state to 'User Binding'
(814) _ldap_extn-state 5 (User Binding)
(429) fthand_ldap_build_userbind_req-Trying DN 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
(194) _ldap_build_bind_req-Binding to 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
(802) fthand_ldap_send-sending 100 bytes to 10.0.1.10
***** fthand_ldap_send-request is sent. ID 4
```

Examine the partial debug output shown in the exhibit. Which two statements about the debug output are true? (Choose two.)

A. The connection to the LDAP server timed out.

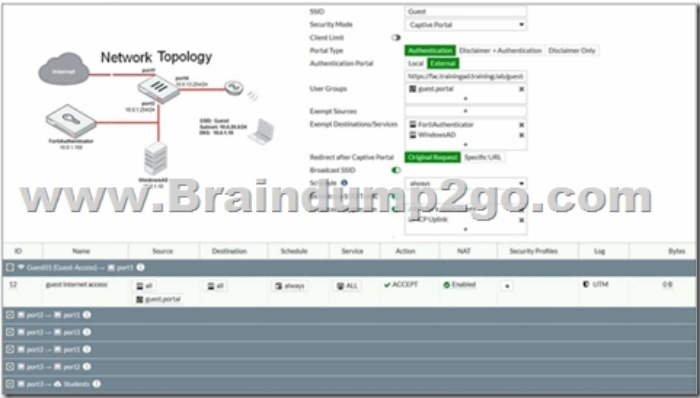
B. The user authenticated successfully.

C. The LDAP server is configured to use regular bind.

D. The debug output shows multiple user authentications.

Answer: AD

QUESTION 19 Refer to the exhibit.



The exhibit shows a network topology and SSID settings. FortiGate is configured to use an external captive portal. However, wireless users are not able to see the captive portal login page. Which configuration change should the administrator make to fix the problem?

A. Create a firewall policy to allow traffic from the Guest SSID to FortiAuthenticator and Windows AD devices.
B. Enable the captive-portal-exempt option in the firewall policy with the ID 10.
C. Remove guest.portal user group in the firewall policy.
D. FortiAuthenticator and WindowsAD address objects should be added as exempt sources.

Answer: C

QUESTION 20

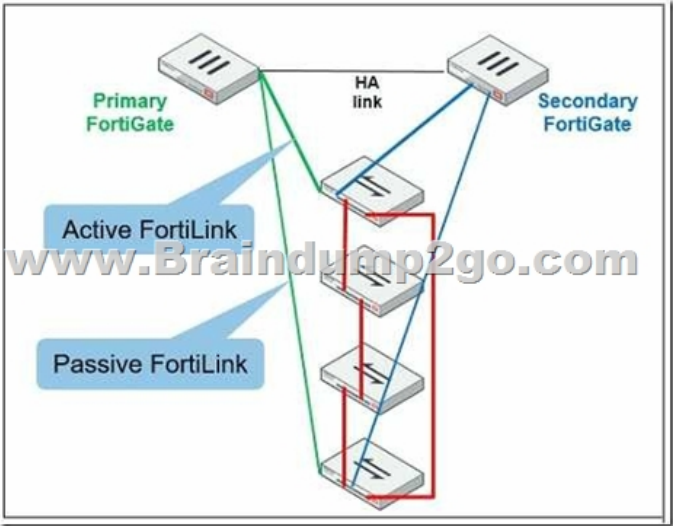
Which CLI command should an administrator use to view the certificate validation process in real-time?

A. diagnose debug application certd -l
B. diagnose debug application fnbamd -l
C. diagnose debug application authd -l
D. diagnose debug application foauthd -l

Answer: A

QUESTION 21

Refer to the exhibit.



The exhibit shows two FortiGate devices in active-passive HA mode, including four FortiSwitch devices connected to a ring. Which two configurations are required to deploy this network topology? (Choose two.)

A. Configure link aggregation interfaces on the FortiLink interfaces.
B. Configure the trunk interfaces on the FortiSwitch devices as MCLAG-ISL.
C. Enable fortlink-split-interface on the FortiLink interfaces.
D. Enable STP on the FortiGate interfaces.

Answer: B

QUESTION 22

Refer to the exhibit.

Debug command

```
# diagnose switch
FS108D3W170023
MAC address
=====
78:2b:cb:d8:36
```

www.B
Port configura

```
config switch-
edit FS108D3
config port
edit port
set le
set di
set ar
end
```

Examine the output of the debug command and port configuration shown in the exhibit. FortiGate learned the MAC address 78:2b:cb:d8:36:68 dynamically. What action does FortiSwitch take if there is an untagged frame coming to port1 with different MAC address? A. The frame is accepted and assigned to the quarantine VLAN. B. The frame is accepted and FortiSwitch will update its mac address table with the new MAC address. C. The frame is dropped. D. The frame is accepted and assigned to the user VLAN. Answer: B QUESTION 23 Which step can be taken to ensure that only FortiAP devices receive IP addresses from a DHCP server on FortiGate? A. Change the interface addressing mode to FortiAP devices. B. Create a reservation list in the DHCP server settings. C. Configure a VCI string value of FortiAP in the DHCP server settings. D. Use DHCP option 138 to assign IPs to FortiAP devices. Answer: C QUESTION 24 Refer to the exhibit.

```
config wireless-controller wtp-profile
edit "Main Networks - FAP-320C"
set comment "Profile with standard networks"
config platform
set type 320C
end
set handoff-rssi 30
set handoff-sta-thresh 30
set ap-country GB
set allowaccess https ssh
set login-passwd-change yes
config radio-1
set band 802.11n,g-only
set channel-utilization enable
set wids-profile "default-wids-apscan-enabled"
set darp enable
set frequency-handoff enable
set ap-handoff enable
set vap-all disable
set vaps "Guest" "Corporate"
set channel "1" "6" "11"
end
config radio-2
set band 802.11ac
set channel-bonding 40MHz
set channel-utilization enable
set wids-profile "default-wids-apscan-enabled"
set darp enable
set frequency-handoff enable
set ap-handoff enable
set vap-all disable
set vaps "Guest" "Corporate"
set channel "36" "44" "52"
end
next
end
```

In the WTP profile configuration shown in the exhibit, the AP profile is assigned to two FAP-320 APs that are installed in an open plan office. The first AP has 32 clients associated to the 5GHz radios and 22 clients associated to the 2.4GHz radio. The second AP has 12 clients associated to the 5GHz radios and 20 clients associated to the 2.4GHz radio. A dual band-capable client enters the office near the first AP and the first AP measures the new client at -33 dBm signal strength. The second AP measures the new client at -43 dBm signal strength. If the new client attempts to connect to the corporate wireless network, to which AP radio will the client be associated? A. The second AP 5GHz interface. B. The first AP 2.4GHz interface. C. The first AP 5GHz interface. D. The second AP 2.4GHz interface. Answer: A QUESTION 25 An administrator is deploying APs that are connecting over an IPsec network. All APs have been configured to connect to FortiGate manually. FortiGate can discover the APs and authorize them. However, FortiGate is unable to establish CAPWAP tunnels to manage the APs. Which configuration setting can the administrator perform to resolve the problem? A. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation. B. Enable CAPWAP administrative access on the IPsec interface. C. Upgrade the FortiAP firmware image to ensure compatibility with the FortiOS version. D. Assign a custom AP profile for the remote APs with the set mpls-connection option enabled. Answer: C QUESTION 26 Refer to the exhibit.

```
> Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on 0
> Ethernet II, Src: Vmware_96:70:b5 (00:50:56:96:70:b5), Dst: Vmware_96:d8:76 (00:50:56:96:d8:76)
> Internet Protocol Version 4, Src: 10.0.1.254, Dst: 10.0.1.150
> User Datagram Protocol, Src Port: 48704, Dst Port: 1812
> RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x96 (150)
  Length: 122
  Attribute Value Pairs
    > AVP: l=18 t=User-Name(1): S1240P3X16008048
    > AVP: l=19 t=User-Name(1): 00-E0-4C-36-00-5E
    > AVP: l=34 t=User-Password(2): Encrypted
    > AVP: l=6 t=User-Port-Type(61): Ethernet(15)
    > AVP: l=19 t=Calling-Station-Id(31): 00-E0-4C-36-00-5E
    > AVP: l=6 t=Service-Type(6): Call-Check(10)
```

Examine the packet capture shown in the exhibit, which contains a RADIUS access request packet sent by FortiSwitch to a RADIUS server. Why does the User-Name field in the RADIUS access request packet contain a MAC address? A. The FortiSwitch

interface is configured for 802.1X port authentication with MAC address bypass, and the connected device does not support 802.1X.
B. FortiSwitch authenticates itself using its MAC address as the user name.
C. The connected device is doing machine authentication.
D. FortiSwitch is replying to an access challenge packet sent by the RADIUS server and requesting the client MAC address.
Answer: A
Resources From: 1. 2020 Latest Braindump2go NSE7_SAC-6.2 Exam Dumps (PDF & VCE) Free Share:
<https://www.braindump2go.com/nse7-sac-6-2.html> 2. 2020 Latest Braindump2go NSE7_SAC-6.2 PDF and NSE7_SAC-6.2 VCE Dumps Free Share: <https://drive.google.com/drive/folders/1qyTXA7fU94w8fevo6brflQWxHg-aBTX5?usp=sharing> 3. 2020 Free Braindump2go NSE7_SAC-6.2 PDF Download:
[https://www.braindump2go.com/free-online-pdf/NSE7_SAC-6.2-PDF-Dumps\(12-22\).pdf](https://www.braindump2go.com/free-online-pdf/NSE7_SAC-6.2-PDF-Dumps(12-22).pdf)
[https://www.braindump2go.com/free-online-pdf/NSE7_SAC-6.2-VCE-Dumps\(1-11\).pdf](https://www.braindump2go.com/free-online-pdf/NSE7_SAC-6.2-VCE-Dumps(1-11).pdf) Free Resources from Braindump2go, We Devoted to Helping You 100% Pass All Exams!