NSE7_SAC-6.2^{Q&As}

Fortinet NSE 7 - Secure Access 6.2

Pass Fortinet NSE7_SAC-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse7_sac-6-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Examine the following RADIUS configuration:

```
config user radius
  edit "FAC-Lab"
    set server "10.0.1.150"
    set secret ENC XXX
    set nas-ip 10.1.0.254
next
```

An administrator has configured a RADIUS server on FortiGate that points to FortiAuthenticator. FortiAuthenticator is acting as an authentication proxy and is configured to relay all authentication requests to a remote Windows AD server using LDAP.

While testing the configuration, the administrator notices that the diagnose test authservercommand works with PAP, however, authentication requests fail when using MSCHAPv2.

Which two changes should the administrator make to get MSCHAPv2 to work? (Choose two.)

A. Force FortiGate to use the PAP authentication method in the RADIUS server configuration.

B. Change the remote authentication server from LDAP to RADIUS on FortiAuthenticator.

C. Use MSCHAP instead of using MSCHAPv2

D. Enable Windows Active Directory Domain Authentication on FortiAuthenticator to add FortiAuthenticator to the Windows domain.

Correct Answer: BD

Reference: https://docs.fortinet.com/document/fortiauthenticator/6.0.0/administration-guide/641286/ remote-authentication-servers

---

QUESTION 2

Refer to the exhibit.

Examine the partial debug output shown in the exhibit.

```
FortiGate # diagnose test authserver ldap Training-Lab student password
[2168] handle_req-Rcvd auth req 1584903618 for student in Training-Lab opt=0000001b prot=0
[358] __compose_group_list_from_req-Group 'Training-Lab'
[608] fnbamd_pop3_start-student
[1038]   fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server 'Training-Lab'
[1544] fnbamd_ldap_init-search filter is: sAMAccountName=student
[1553] fnbamd_ldap_init-search base is: cn=users,dc=trainingad,dc=training,dc=lab
[973]   fnbamd_ldap_dns_cb-Resolved Training-Lab(idx 0) to 10.0.1.10
[1021]   fnbamd_ldap_dns_cb-Still connecting.
[517] create_auth_session-Total 1 server(s) to try
[939]   ldap_connect-tcps_connect(10.0.1.10) is established.
[814]   ldap_rxtx-state 3(Admin Binding)
[196]   ldap_build_bind_req-Binding to 'CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab'
[852] fnbamd_ldap_send-sending 80 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 1
[814]   ldap_rxtx-state 4(Admin Bind resp)
[1056] fnbamd_ldap_recv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:1, type:bind
[791] fnbamd_ldap_parse_response-ret=0
[881]   ldap_rxtx-Change state to 'DN search'
[814]   ldap_rxtx-state 11(DN search)
[584] fnbamd_ldap_build_dn_search_req-base:'cn=users,dc=trainingad,dc=training,dc=lab' filter:sAMAccountName=student
[852] fnbamd_ldap_send-sending 99 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 2
[814]   ldap_rxtx-state 12(DN search resp)
[1056] fnbamd_ldap_recv-Response len: 69, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-entry
[791] fnbamd_ldap_parse_response-ret=0
[1095]   fnbamd_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] fnbamd_ldap_recv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-result
[791] fnbamd_ldap_parse_response-ret=0
[881]   ldap_rxtx-Change state to 'User Binding'
[814]   ldap_rxtx-state 5(User Binding)
[429] fnbamd_ldap_build_userbind_req-Trying DN 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[196]   ldap_build_bind_req-Binding to 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[852] fnbamd_ldap_send-sending 105 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 3
[814]   ldap_rxtx-state 6(User Bind resp)
[1056] fnbamd_ldap_recv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:3, type:bind
[791] fnbamd_ldap_parse_response-ret=0
[881]   ldap_rxtx-Change state to 'Attr query'
[814]   ldap_rxtx-state 7(Attr query)
[482] fnbamd_ldap_build_attr_search_req-Adding attr 'memberOf'
[194] fnbamd_ldap_build_attr_search_req-base:'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab' filter:cn=*
[852] fnbamd_ldap_send-sending 128 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 4
```

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.

Correct Answer: BC

QUESTION 3

Refer to the exhibit.

Examine the packet capture shown in the exhibit, which contains a RADIUS access request packet sent by FortiSwitch to a RADIUS server.

```
> Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
> 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
      Authenticator: 49a700a9981a2eb044bf811f482412a0
      [The response to this request is in frame 2]
   ∨ Attribute Value Pairs
      > AVP: l=18 t=NAS-Identifier(32): S124DP3X16008048
      > AVP: l=19 t=User-Name(1): 00-E0-4C-36-0D-5E
      > AVP: l=34 t=User-Password(2): Encrypted
      > AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
      > AVP: l=19 t=Calling-Station-Id(31): 00-E0-4C-36-0D-5E
      > AVP: l=6 t=Service-Type(6): Call-Check(10)
```

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.

Correct Answer: D

QUESTION 4

Refer to the exhibit.

Examine the network topology shown in the exhibit.
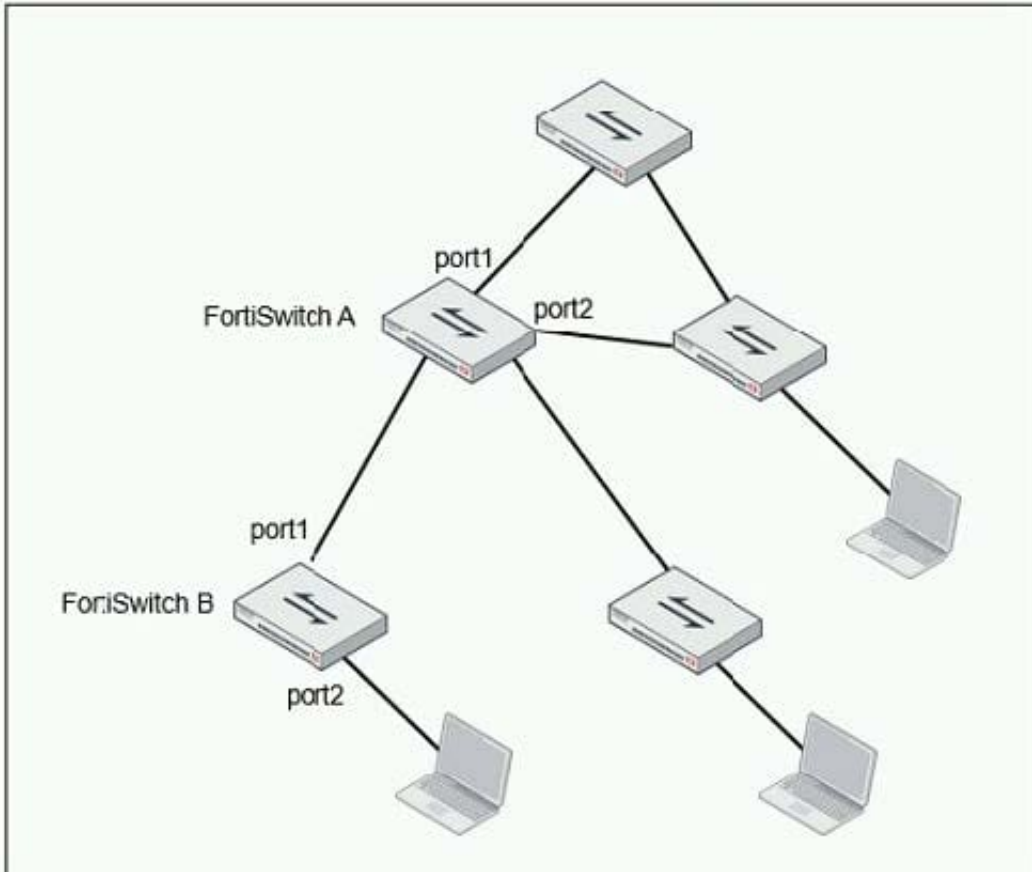
Which port should have root guard enabled?

A. FortiSwitch A, port2

B. FortiSwitch A, port1

C. FortiSwitch B, port1

D. FortiSwitch B, port2

Correct Answer: A

Reference: https://docs.fortinet.com/document/fortiswitch/6.4.2/administration-guide/364614/spanningtree-protocol

---

QUESTION 5

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.

Correct Answer: A

Latest NSE7_SAC-6.2 Dumps

NSE7_SAC-6.2 VCE Dumps

NSE7_SAC-6.2 Practice Test