

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

Refer to the exhibit.

```
FortiGate # diagnose switch-controller switch-info 802.1X
Managed Switch: S224EPTF18001736
   port2 : Mode: port-based (mac-by-pass disable)
           Link: Link up
           Port State: unauthorized: ( )
           Dynamic Authorized Vlan: 0
           EAP pass-through mode : Enable
           Quarantine VLAN (4093) detection : Enable
           Native Vlan: 10
           Allowed Vlan list: 10,4093
           Untagged Vlan list: 4093
           Guest VLAN :
           Auth-Fail Vlan :
           Sessions info:
           00:09:0f:02:02:02
                                 Type=802.1x,,state=AUTHENTICATING,etime=0,eap_cnt=0 params:reAuth=3600
```

A host machine connected to port2 on FortiSwitch cannot connect to the network. All ports on FortiSwitch are assigned a security policy to enforce 802.1X port authentication. While troubleshooting the issue, the administrator runs the debug command and obtains the output shown in the exhibit.

Which two scenarios are the likely cause of this issue? (Choose two.)

- A. The host machine is not configured for 802.1X port authentication.
- B. The host machine does not support 802. 1X authentication.
- C. The host machine is quarantined due to a security incident.
- D. The host machine is configured with wrong VLAN ID.

Correct Answer: AB

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD46428

QUESTION 2

Refer to the exhibit.

Examine the configuration of the FortiSwitch security policy profile.



Edit FortiSwitch Security Poli	су			
Name		Students		
Security mode		Port-based N	/AC-based	
User groups		Wired-User	rs +	×
Guest VLAN (0	₫ guest		•
Guest authentication delay		120		second(s
Authentication fail VLAN	0	auth-fail auth-fa		-
MAC authentication bypass	0			
EAP pass-through	0			
Override RADIUS timeout	•			

If the security profile shown in the exhibit is assigned on the FortiSwitch port for 802.1X.port authentication, which statement is correct?

- A. Host machines that do support 802.1X authentication, but have failed authentication, will be assigned the guest VLAN.
- B. All unauthenticated users will be assigned the auth-fail VLAN.
- C. Authenticated users that are part of the wired-users group will be assigned the guest VLAN.
- D. Host machines that do not support 802.1X authentication will be assigned the guest VLAN.

Correct Answer: C

QUESTION 3

802.1X port authentication is enabled on only those ports that the FortiSwitch security policy is assigned to.

Which configurable items are available when you configure the security policy on FortiSwitch? (Choose two.)

- A. FSSO groups
- B. Security mode
- C. User groups
- D. Default guest group

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

2024 Latest pass2lead NSE7_SAC-6.2 PDF and VCE dumps Download

Correct Answer: BC

QUESTION 4

Examine the following output from the FortiLink real-time debug.

FortiGate diagnose debug application fortilinkd 3

fl_node_apply_switch_port_fgt_properties_update_with_portname[977]:port properties are different for
port(port9) in switch(FS108D3W17002387) old(0x1) new(0x1)o-peer-port() n-peer-port(port2) o-peer-device() npeer-device(FGVMEVBB6ITDAO1B)

... flp_event_handler[605]:node: port2 received event 110 state FL_STATE_READY switchname flags 0x26a

... flp_event_handler[605]:node: port2 received event 111 state FL_STATE_READY switchname flags 0x26a

... flp_send_pkt[339]:pkt-sent {type(5) flag=0xe2 node(port2) sw(port2) len(26)smac: 0: c:29:51:dd:a0
dmac:70:4c:a5:24:ba:4f

Based on the output, what is the status of the communication between FortiGate and FortiSwitch?

- A. FortiGate is unable to authorize the FortiSwitch.
- B. FortiGate is unable to establish FortiLink tunnel to manage the FortiSwitch.
- C. FortiGate is unable to located a previously managed FortiSwitch.
- D. The FortiLink heartbeat is up.

Correct Answer: D

QUESTION 5

Refer to the exhibit.

Examine the output of the debug command and port configuration shown in the exhibit.



Debug command output

```
# diagnose switch-controller switch-info mac-table
FS108D3W17002387 0:
```

MAC address Interface vlan

78:2b:cb:d8:36:68 port1 4094

Port configuration

```
config switch-controller managed-switch
edit FS108D3W17002387
config ports
edit port1
set learning-limit 1
set discard-mode all-tagged
set arp-inspection-trust untrusted
end
```

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 will 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.

Correct Answer: A

NSE7 SAC-6.2 PDF Dumps

NSE7 SAC-6.2 Exam

Questions

NSE7_SAC-6.2 Braindumps