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.geekcert.com/nse7_sac-6-2.html

100% Passing Guarantee
100% Money Back Assurance

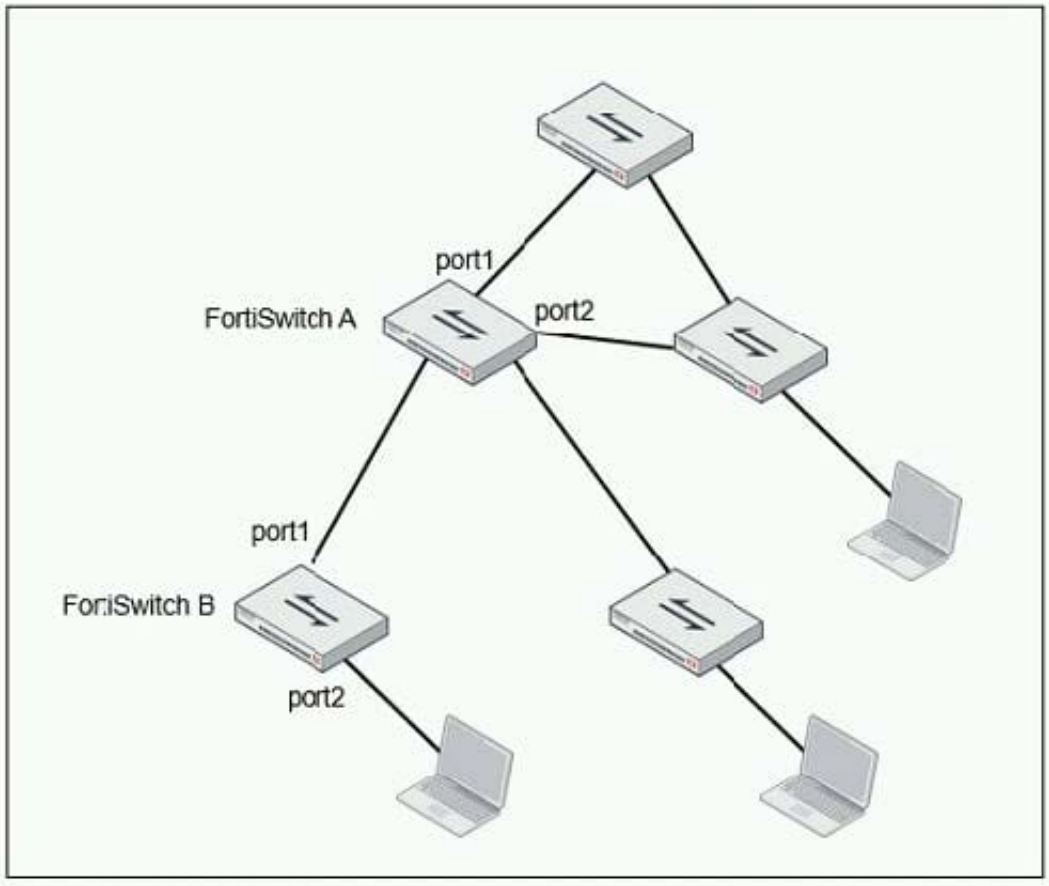
Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit.

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 2

What action does FortiSwitch take when it receives a loop guard data packet (LGDP) that was sent by itself?

A. The receiving port is shut down.

B. The sending port is shut down

C. The receiving port is moved to the STP blocking state.

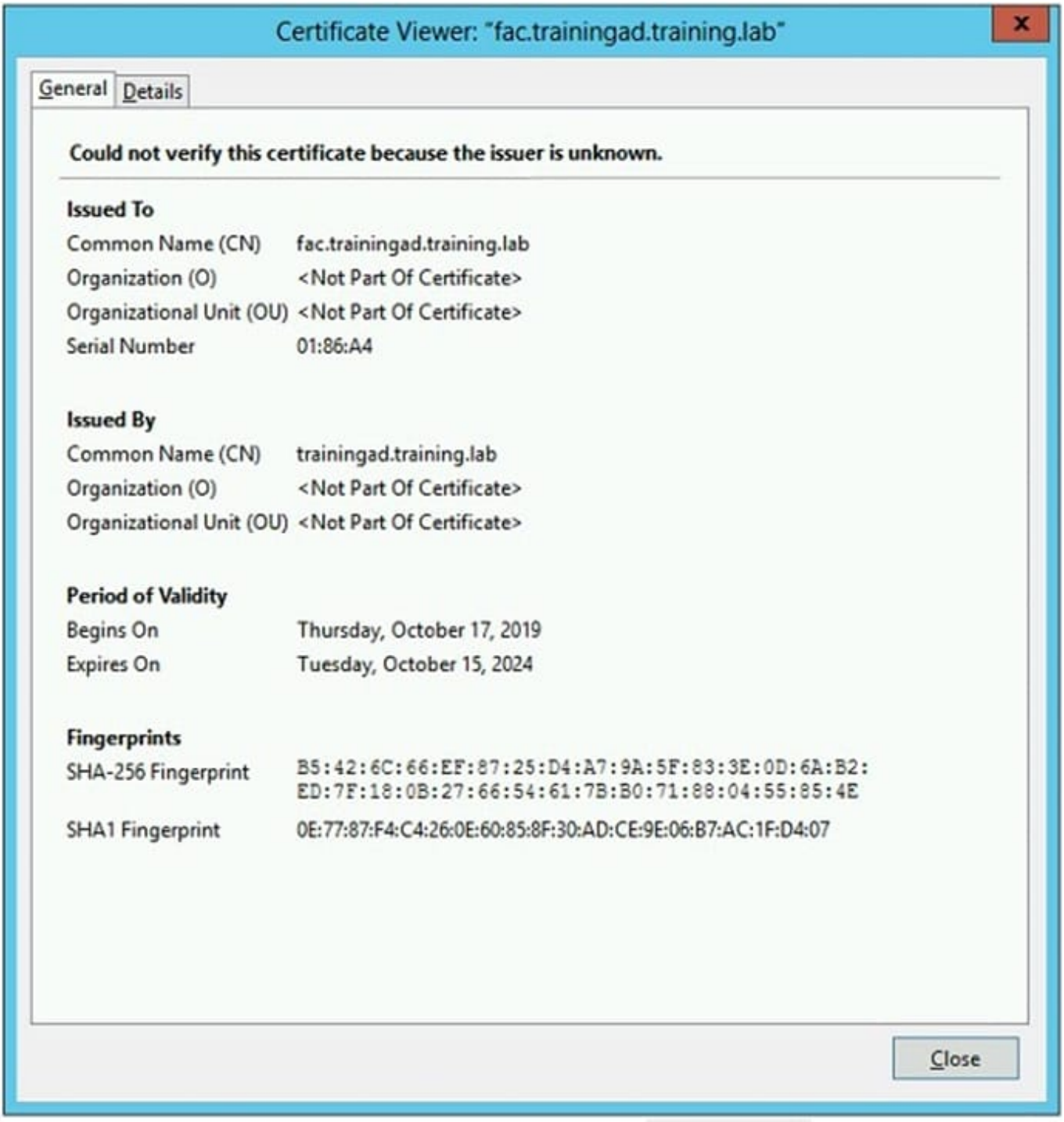
D. The sending port is moved to the STP blocking state

Correct Answer: B

Reference: https://www.scribd.com/document/468940309/Secure-Access-6-0-Study-Guide-Online-pdf

QUESTION 3

Refer to the exhibit showing certificate values.



Wireless guest users are unable to authenticate because they are getting a certificate error while loading the captive portal login page. This URL string is the HTTPS POST URL guest wireless users see when attempting to access the network using the web browser:

https://fac.trainingad.training.com/guests/login/?loginandpost=https://auth.trainingad.training.1ab:1003/fgtauthandmagic=000a038293d1f411andusermac=b8:27:eb:d8:50:02andapmac=70:4c:a5:9d:0d:28andapip=10.10.100.2anduserip=10.0.3.1andssid=Guest03andapname=PS221ETF18000148andbssid=70:4c:a5:9d:0d:30

Which two settings are the likely causes of the issue? (Choose two.)

A. The external server FQDN is incorrect.

B. The FortiGate authentication interface address is using HTTPS.

C. The wireless user\\'s browser is missing a CA certificate.

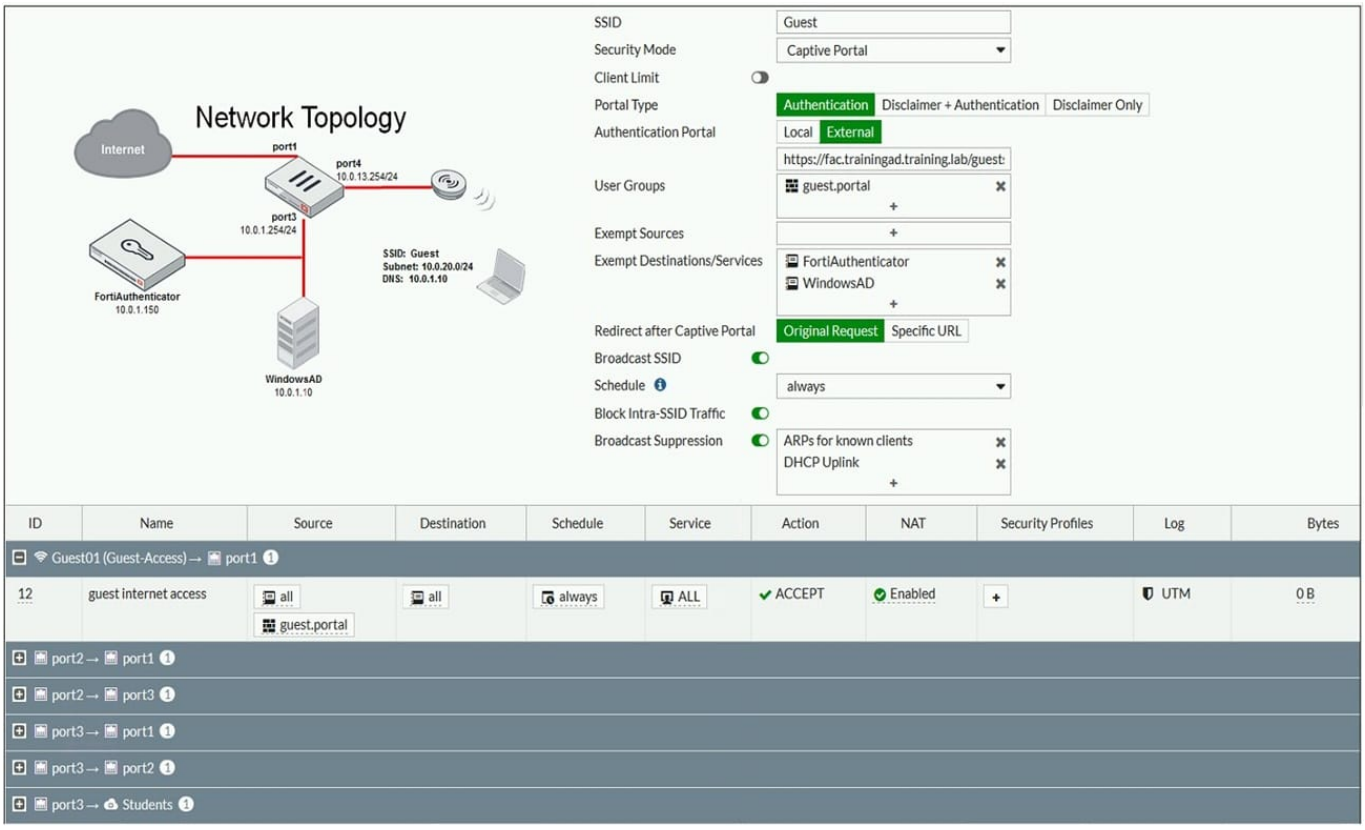
D. The user address is not in DDNS form.

Correct Answer: AC

QUESTION 4

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-exemptoption 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.

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/868644/captive-portals

QUESTION 5

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.

Correct Answer: C