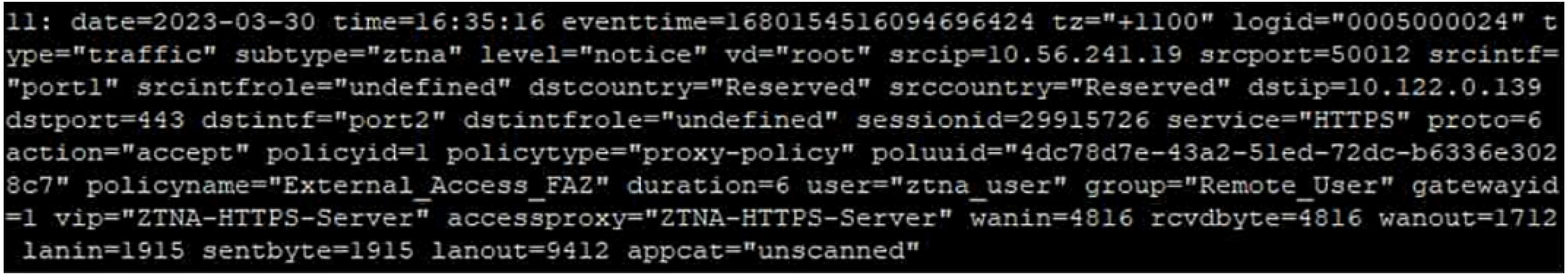
Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 1

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Refer to the exhibit.



```
11: date=2023-03-30 time=16:35:16 eventtime=1680154516094696424 tz="+1100" logid="0005000024" t
ype="traffic" subtype="ztna" level="notice" vd="root" srcip=10.56.241.19 srcport=50012 srcintf=
"port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved" dstip=10.122.0.139
dstport=443 dstintf="port2" dstintfrole="undefined" sessionid=29915726 service="HTTPS" proto=6
action="accept" policyid=1 policytype="proxy-policy" poluuid="4dc78d7e-43a2-51ed-72dc-b6336e302
8c7" policyname="External_Access_FAZ" duration=6 user="ztna_user" group="Remote_User" gatewayid
=1 vip="ZTNA-HTTPS-Server" accessproxy="ZTNA-HTTPS-Server" wanin=4816 rcvdbyte=4816 wanout=1712
 lanin=1915 sentbyte=1915 lanout=9412 appcat="unscanned"
```

Based on the ZTNA logs provided, which statement is true?

A. The Remote_User ZTNA tag has matched the ZTNA rule.

B. An authentication scheme is configured.

C. The external IP for ZTNA server is 10.122.0.139.

D. Traffic is allowed by firewall policy 1.

Show Suggested Answer

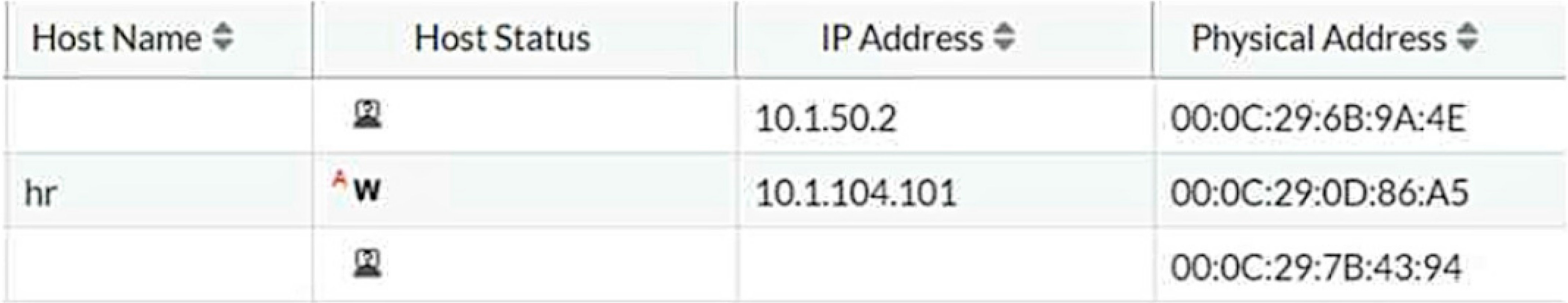
Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 2

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Refer to exhibit.



Host Name	Host Status	IP Address	Physical Address
	👤	10.1.50.2	00:0C:29:6B:9A:4E
hr	W	10.1.104.101	00:0C:29:0D:86:A5
	👤		00:0C:29:7B:43:94

Which statement is true about the hr endpoint?

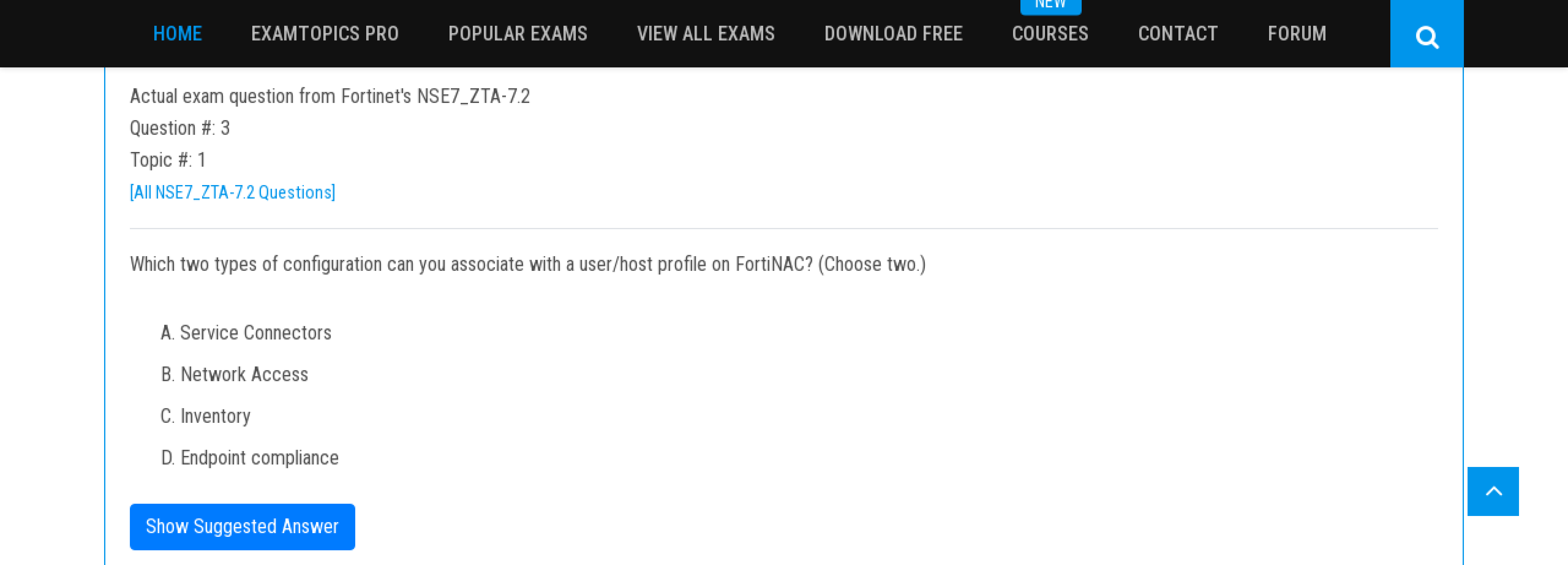
A. The endpoint is a rogue device.

B. The endpoint is disabled.

C. The endpoint is unauthenticated.

D. The endpoint has been marked at risk.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 3

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Which two types of configuration can you associate with a user/host profile on FortiNAC? (Choose two.)

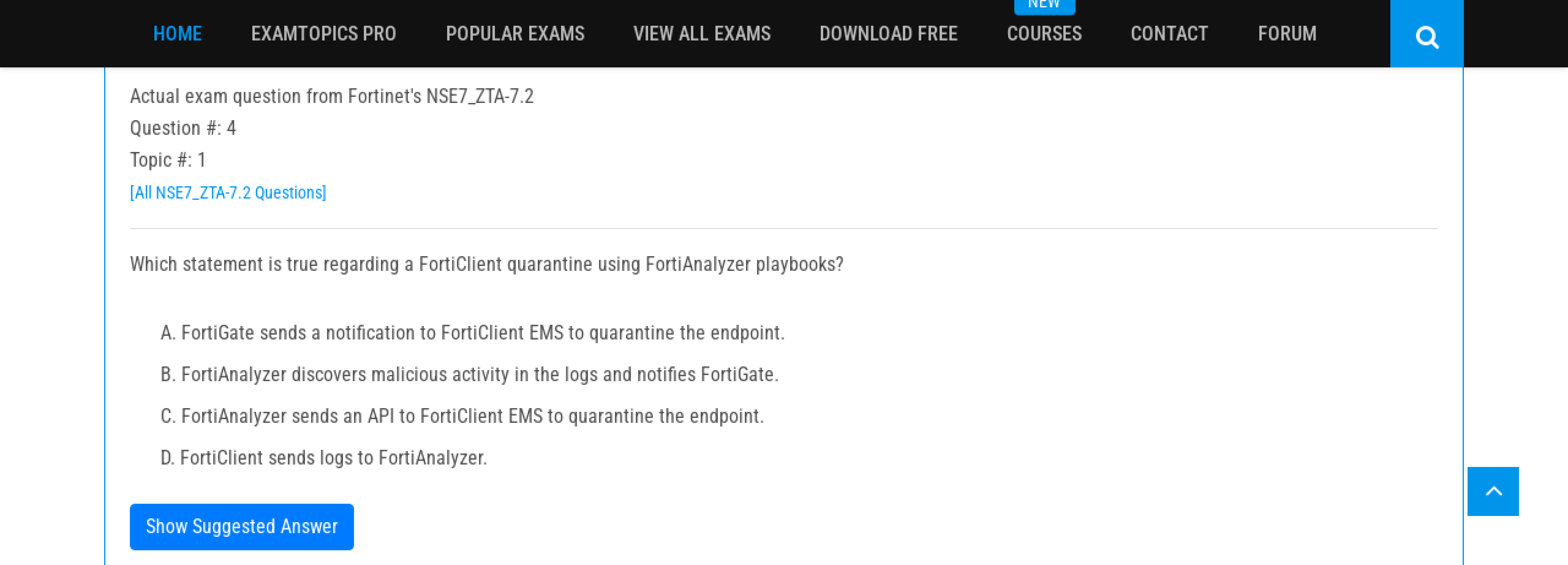
A. Service Connectors

B. Network Access

C. Inventory

D. Endpoint compliance

Show Suggested Answer



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 4

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Which statement is true regarding a FortiClient quarantine using FortiAnalyzer playbooks?

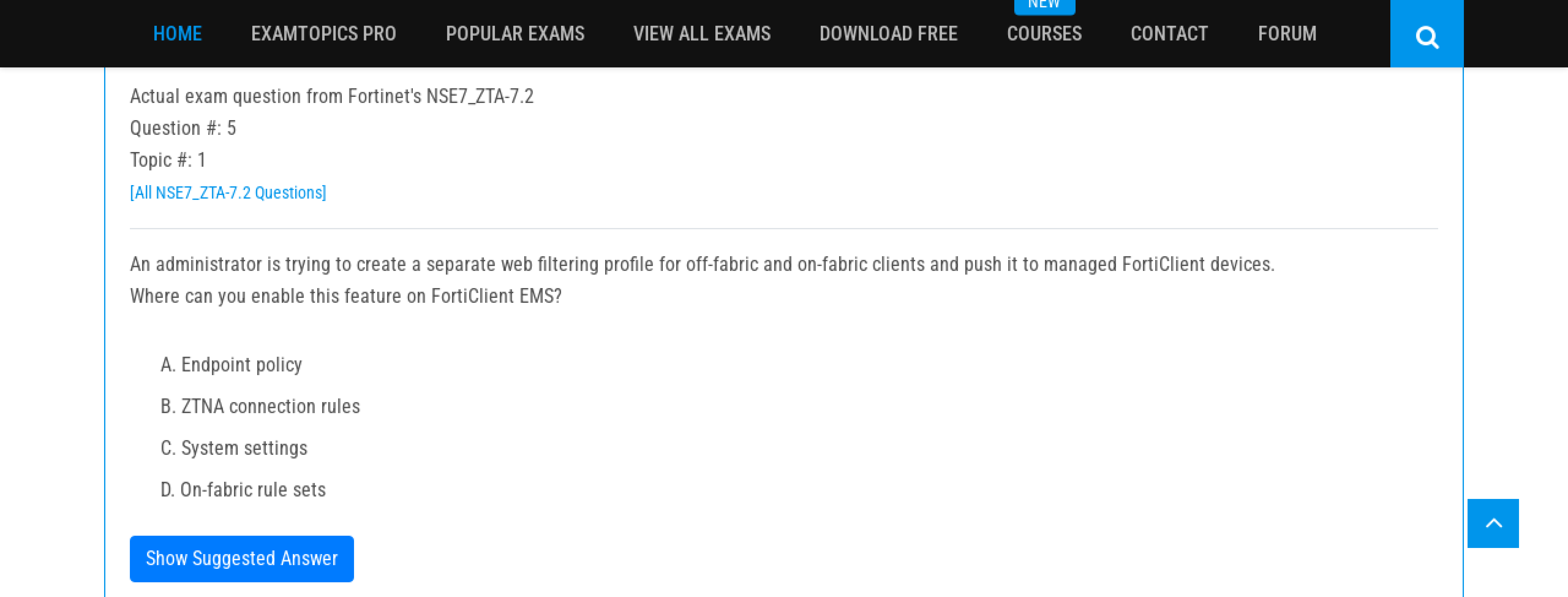
A. FortiGate sends a notification to FortiClient EMS to quarantine the endpoint.

B. FortiAnalyzer discovers malicious activity in the logs and notifies FortiGate.

C. FortiAnalyzer sends an API to FortiClient EMS to quarantine the endpoint.

D. FortiClient sends logs to FortiAnalyzer.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 5

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

An administrator is trying to create a separate web filtering profile for off-fabric and on-fabric clients and push it to managed FortiClient devices.
Where can you enable this feature on FortiClient EMS?

A. Endpoint policy

B. ZTNA connection rules

C. System settings

D. On-fabric rule sets

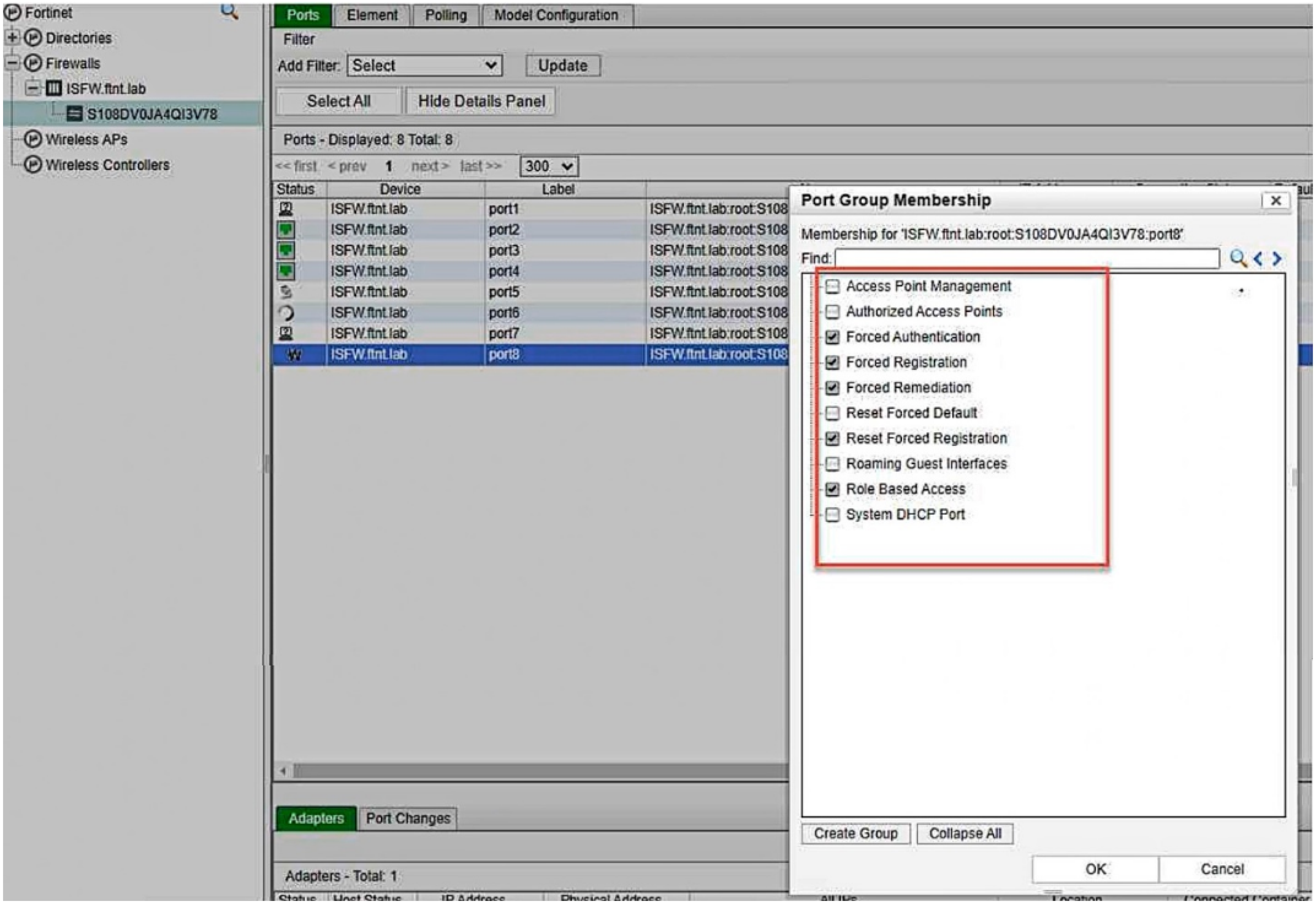
Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 6

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Refer to the exhibit.



Ports - Displayed: 8 Total: 8

Status	Device	Label	
	ISFW.ftnt.lab	port1	ISFW.ftnt.lab:root:S108
	ISFW.ftnt.lab	port2	ISFW.ftnt.lab:root:S108
	ISFW.ftnt.lab	port3	ISFW.ftnt.lab:root:S108
	ISFW.ftnt.lab	port4	ISFW.ftnt.lab:root:S108
	ISFW.ftnt.lab	port5	ISFW.ftnt.lab:root:S108
	ISFW.ftnt.lab	port6	ISFW.ftnt.lab:root:S108
	ISFW.ftnt.lab	port7	ISFW.ftnt.lab:root:S108
	ISFW.ftnt.lab	port8	ISFW.ftnt.lab:root:S108

Port Group Membership

Membership for 'ISFW.ftnt.lab:root:S108DV0JA4QI3V78:port8'

Find:

- ☐ Access Point Management
- ☐ Authorized Access Points
- ☑ Forced Authentication
- ☑ Forced Registration
- ☑ Forced Remediation
- ☐ Reset Forced Default
- ☑ Reset Forced Registration
- ☐ Roaming Guest Interfaces
- ☑ Role Based Access
- ☐ System DHCP Port

Which port group membership should you enable on FortiNAC to isolate rogue hosts?

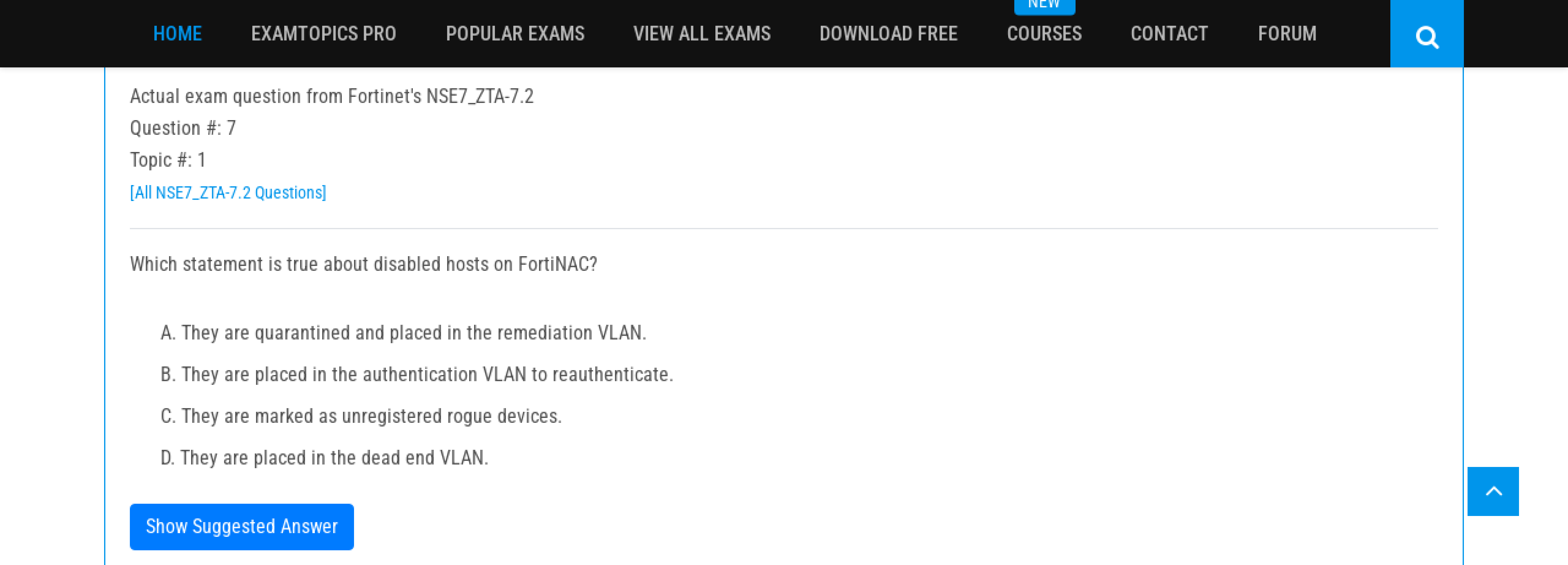
A. Forced Authentication

B. Forced Registration

C. Forced Remediation

D. Reset Forced Registration

Show Suggested Answer



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 7

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Which statement is true about disabled hosts on FortiNAC?

A. They are quarantined and placed in the remediation VLAN.

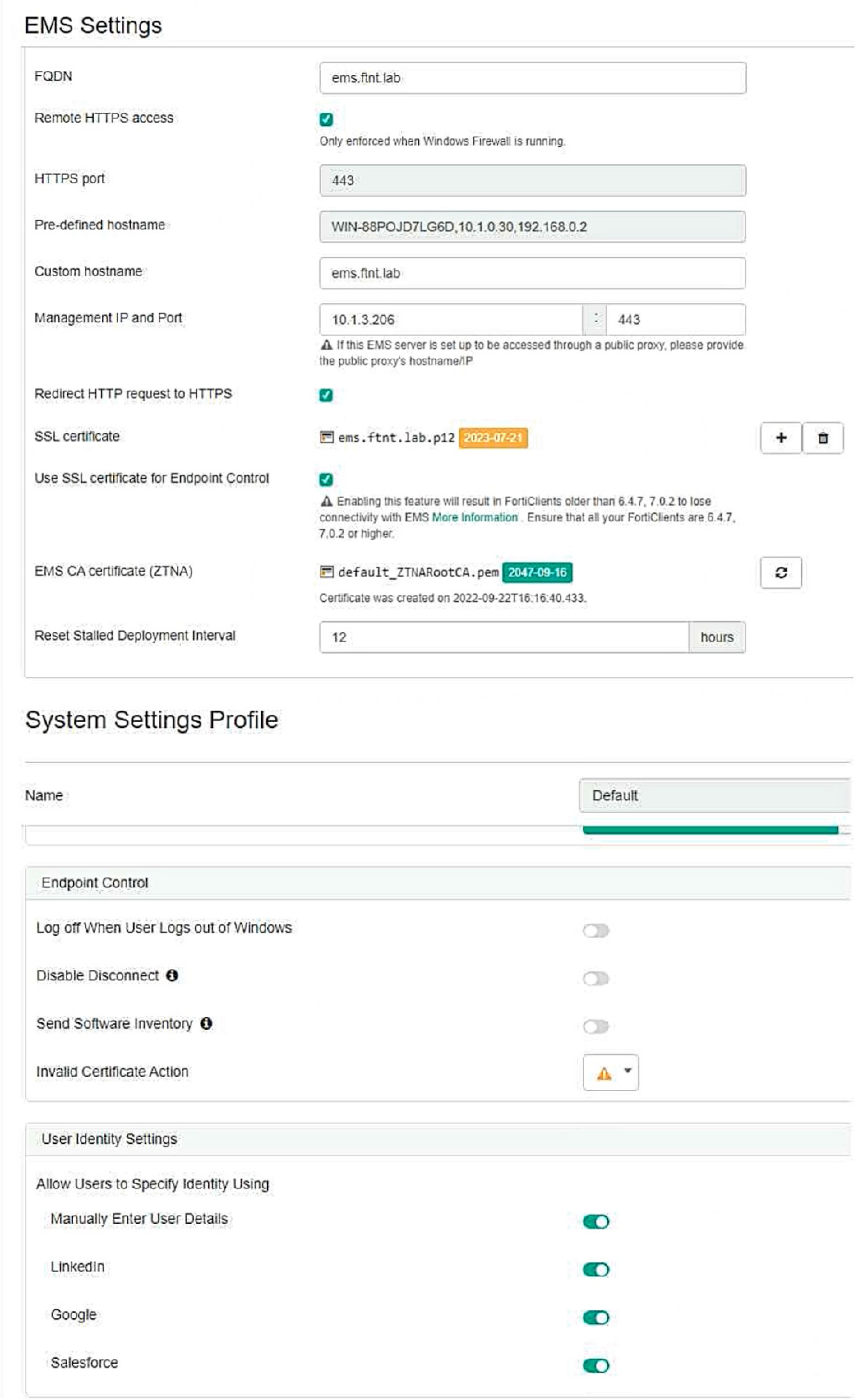
B. They are placed in the authentication VLAN to reauthenticate.

C. They are marked as unregistered rogue devices.

D. They are placed in the dead end VLAN.

Actual exam question from Fortinet's NSE7_ZTA-7.2
Question #: 8
Topic #: 1
[All NSE7_ZTA-7.2 Questions]

Refer to the exhibits.



EMS Settings

FQDN: ems.ftnt.lab

Remote HTTPS access: ☑
Only enforced when Windows Firewall is running.

HTTPS port: 443

Pre-defined hostname: WIN-88POJD7LG6D,10.1.0.30,192.168.0.2

Custom hostname: ems.ftnt.lab

Management IP and Port: 10.1.3.206 : 443
⚠ If this EMS server is set up to be accessed through a public proxy, please provide the public proxy's hostname/IP

Redirect HTTP request to HTTPS: ☑

SSL certificate: ems.ftnt.lab.p12 2023-07-21

Use SSL certificate for Endpoint Control: ☑
⚠ Enabling this feature will result in FortiClients older than 6.4.7, 7.0.2 to lose connectivity with EMS More Information . Ensure that all your FortiClients are 6.4.7, 7.0.2 or higher.

EMS CA certificate (ZTNA): default_ZTNARootCA.pem 2047-09-16
Certificate was created on 2022-09-22T16:16:40.433.

Reset Stalled Deployment Interval: 12 hours

System Settings Profile

Name: Default

Endpoint Control

Log off When User Logs out of Windows: ○
Disable Disconnect: ○
Send Software Inventory: ○
Invalid Certificate Action: ⚠

User Identity Settings

Allow Users to Specify Identity Using
Manually Enter User Details: ●
LinkedIn: ●
Google: ●
Salesforce: ●

Which statement is true about the configuration shown in the exhibit?

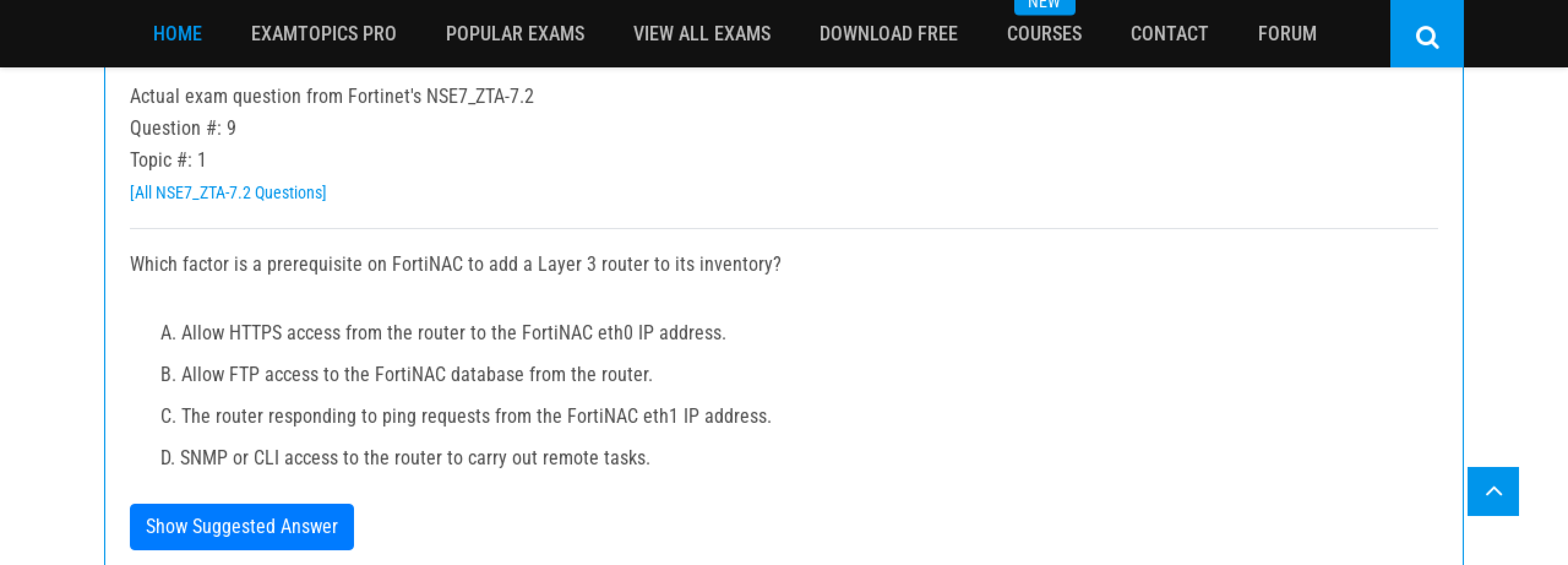
A. The domain that FortiClient is connecting to should match the domain to which the certificate is issued.

B. If the FortiClient EMS server certificate is invalid, FortiClient connects silently.

C. The connection from FortiClient to FortiClient EMS uses TCP and TLS 1.2.

D. default_ZTNARoot CA signs the FortiClient certificate for the SSL connectivity to FortiClient EMS.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 9

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

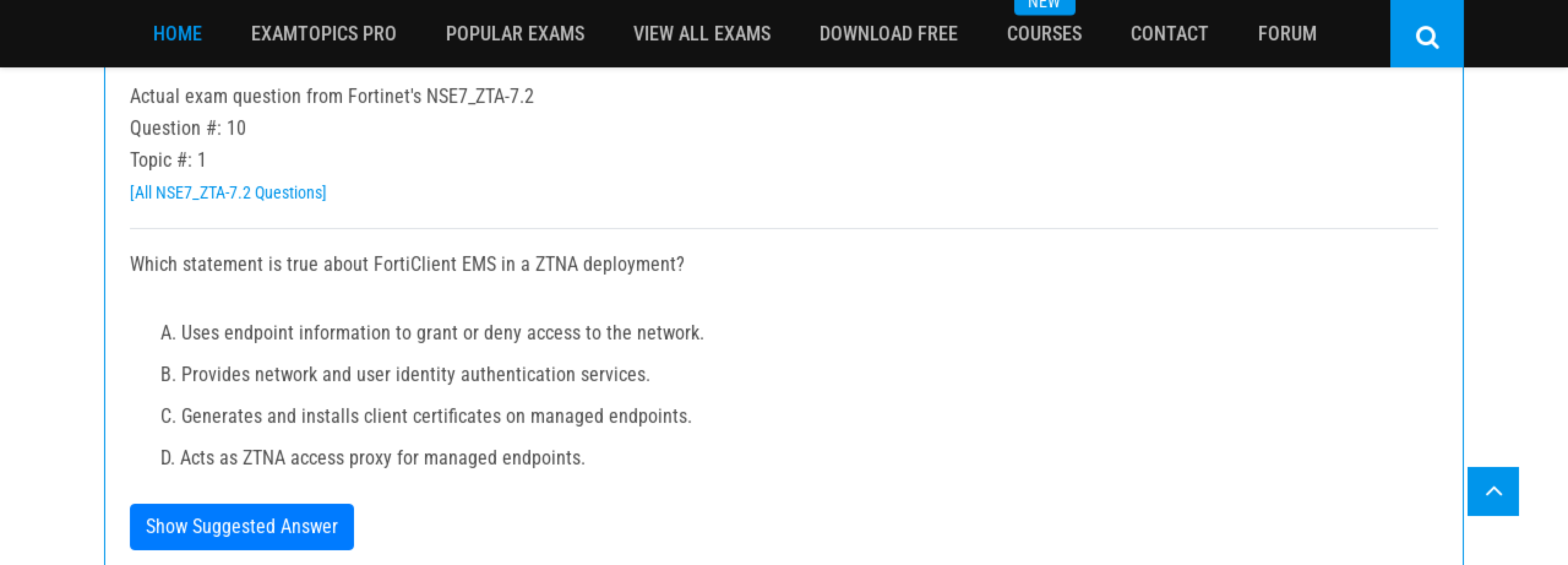
Which factor is a prerequisite on FortiNAC to add a Layer 3 router to its inventory?

A. Allow HTTPS access from the router to the FortiNAC eth0 IP address.

B. Allow FTP access to the FortiNAC database from the router.

C. The router responding to ping requests from the FortiNAC eth1 IP address.

D. SNMP or CLI access to the router to carry out remote tasks.



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 10

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Which statement is true about FortiClient EMS in a ZTNA deployment?

A. Uses endpoint information to grant or deny access to the network.

B. Provides network and user identity authentication services.

C. Generates and installs client certificates on managed endpoints.

D. Acts as ZTNA access proxy for managed endpoints.

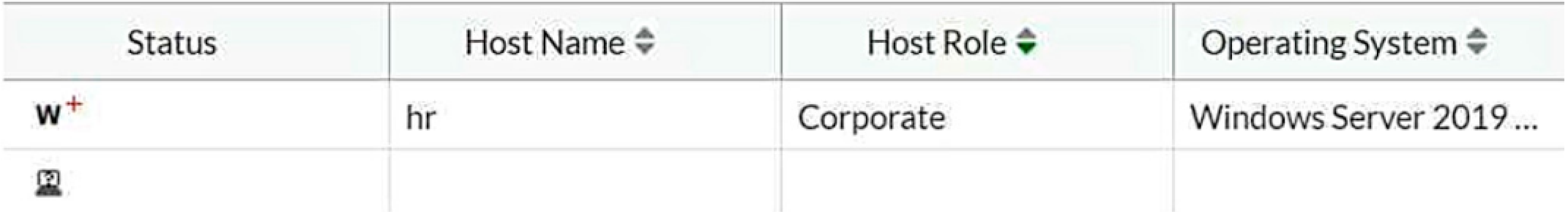
Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 11

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Refer to the exhibit.



Status	Host Name	Host Role	Operating System
w+	hr	Corporate	Windows Server 2019 ...
?			

Which two statements are true about the hr endpoint? (Choose two.)

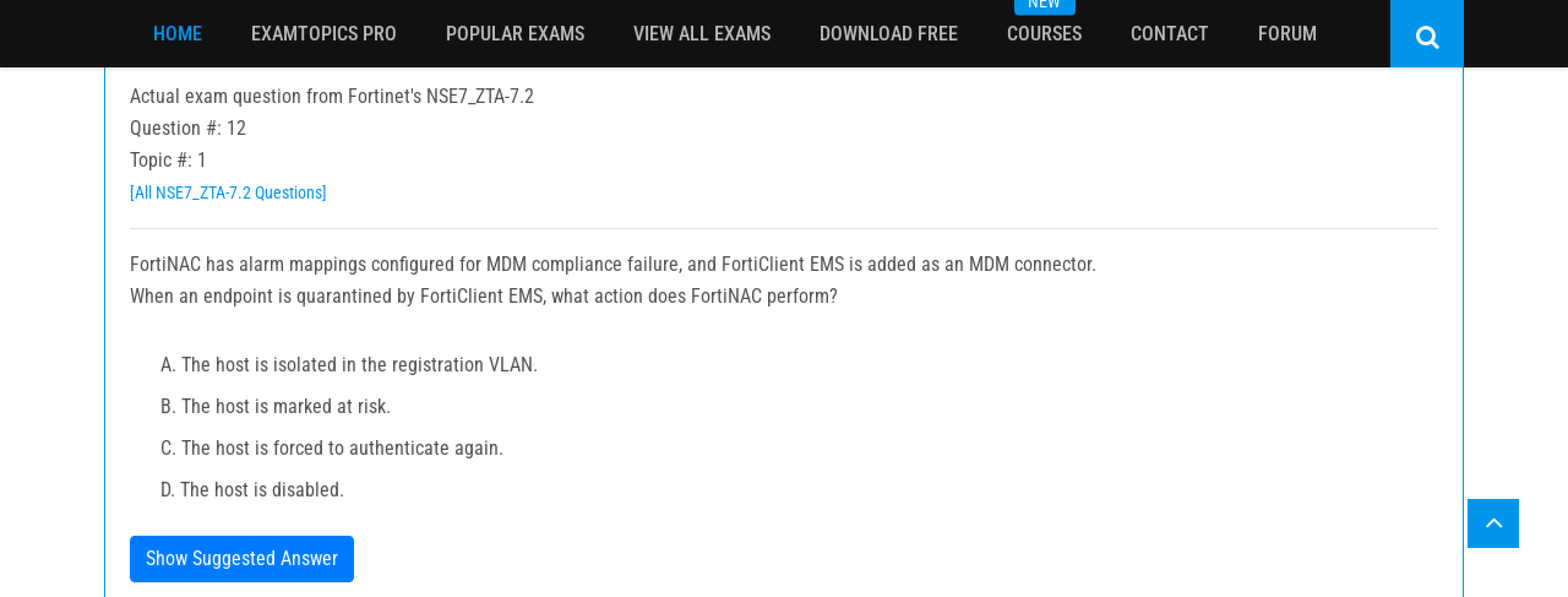
A. The endpoint application inventory could not be retrieved.

B. The endpoint is marked as a rogue device.

C. The endpoint has failed the compliance scan.

D. The endpoint will be moved to the remediation VLAN.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_ZTA-7.2
Question #: 12
Topic #: 1
[All NSE7_ZTA-7.2 Questions]

FortiNAC has alarm mappings configured for MDM compliance failure, and FortiClient EMS is added as an MDM connector.
When an endpoint is quarantined by FortiClient EMS, what action does FortiNAC perform?

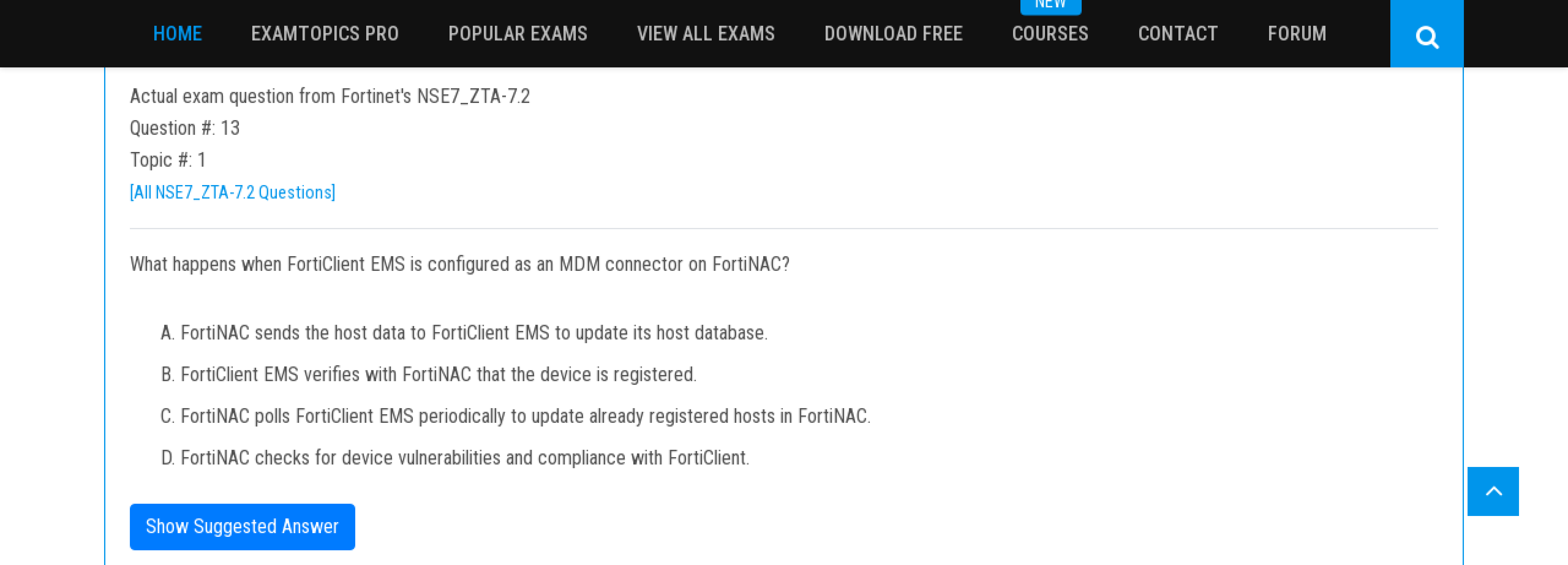
A. The host is isolated in the registration VLAN.

B. The host is marked at risk.

C. The host is forced to authenticate again.

D. The host is disabled.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 13

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

What happens when FortiClient EMS is configured as an MDM connector on FortiNAC?

A. FortiNAC sends the host data to FortiClient EMS to update its host database.

B. FortiClient EMS verifies with FortiNAC that the device is registered.

C. FortiNAC polls FortiClient EMS periodically to update already registered hosts in FortiNAC.

D. FortiNAC checks for device vulnerabilities and compliance with FortiClient.

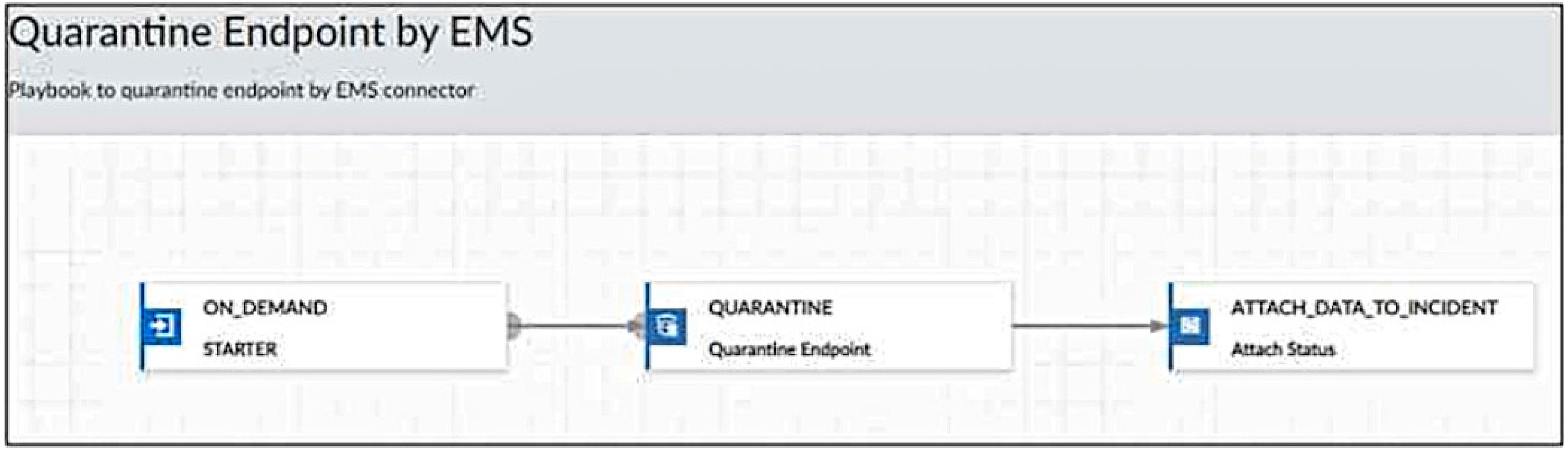
Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 14

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Refer to the exhibit.



Quarantine Endpoint by EMS

Playbook to quarantine endpoint by EMS connector

Which statement is true about the FortiAnalyzer playbook configuration shown in the exhibit?

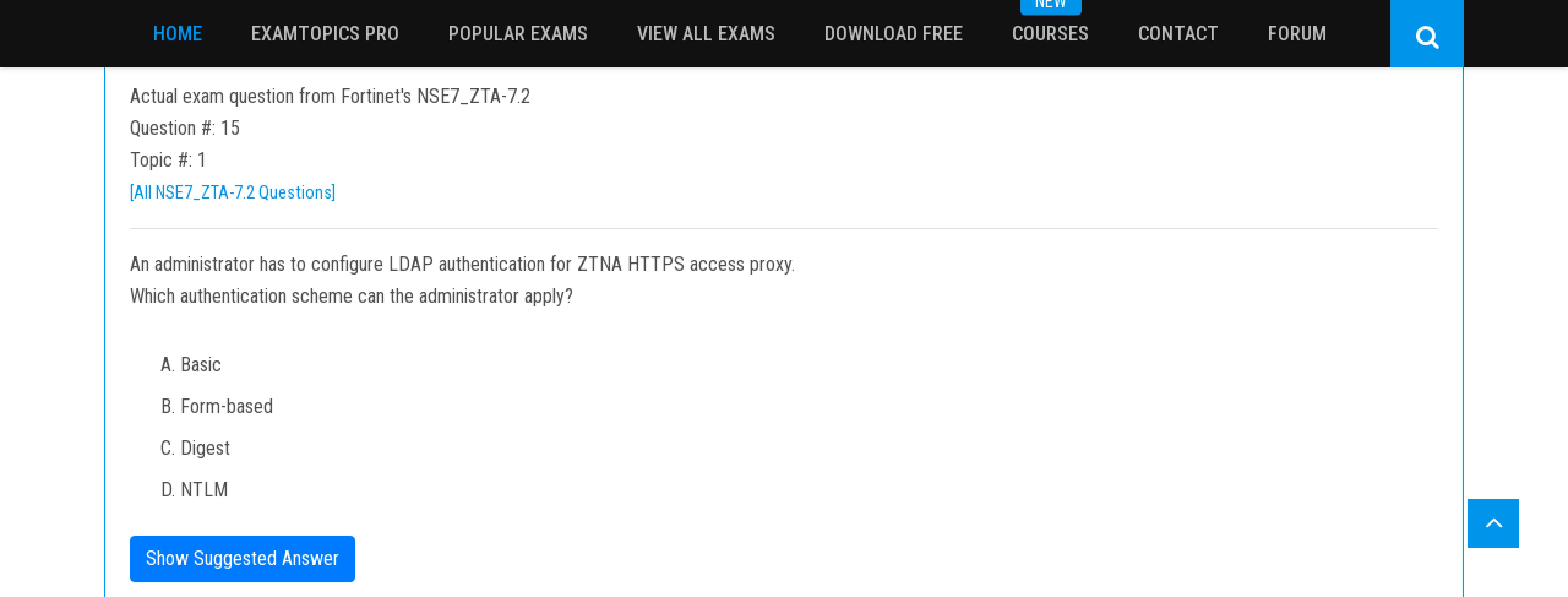
A. The playbook is run on a configured schedule.

B. The playbook is run when an incident is created that matches the filters.

C. The playbook is run when an event is created that matches the filters.

D. The playbook is manually started by an administrator.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 15

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

An administrator has to configure LDAP authentication for ZTNA HTTPS access proxy.

Which authentication scheme can the administrator apply?

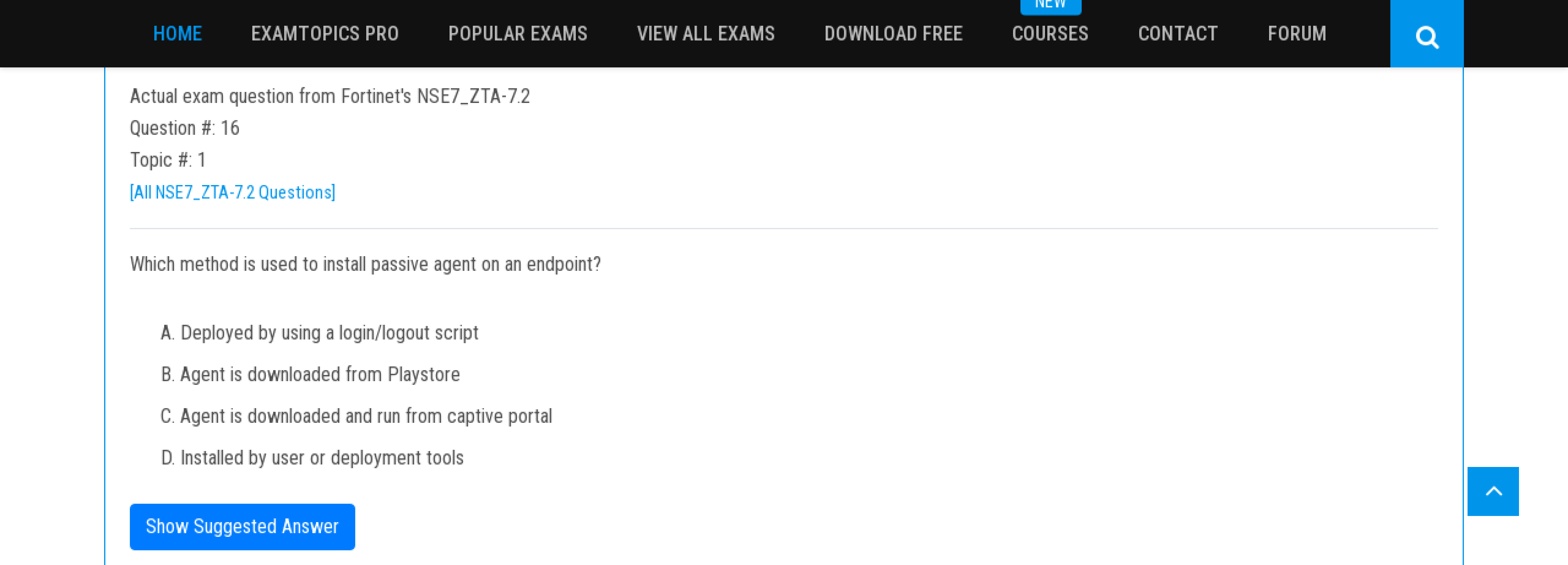
A. Basic

B. Form-based

C. Digest

D. NTLM

Show Suggested Answer



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 16

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

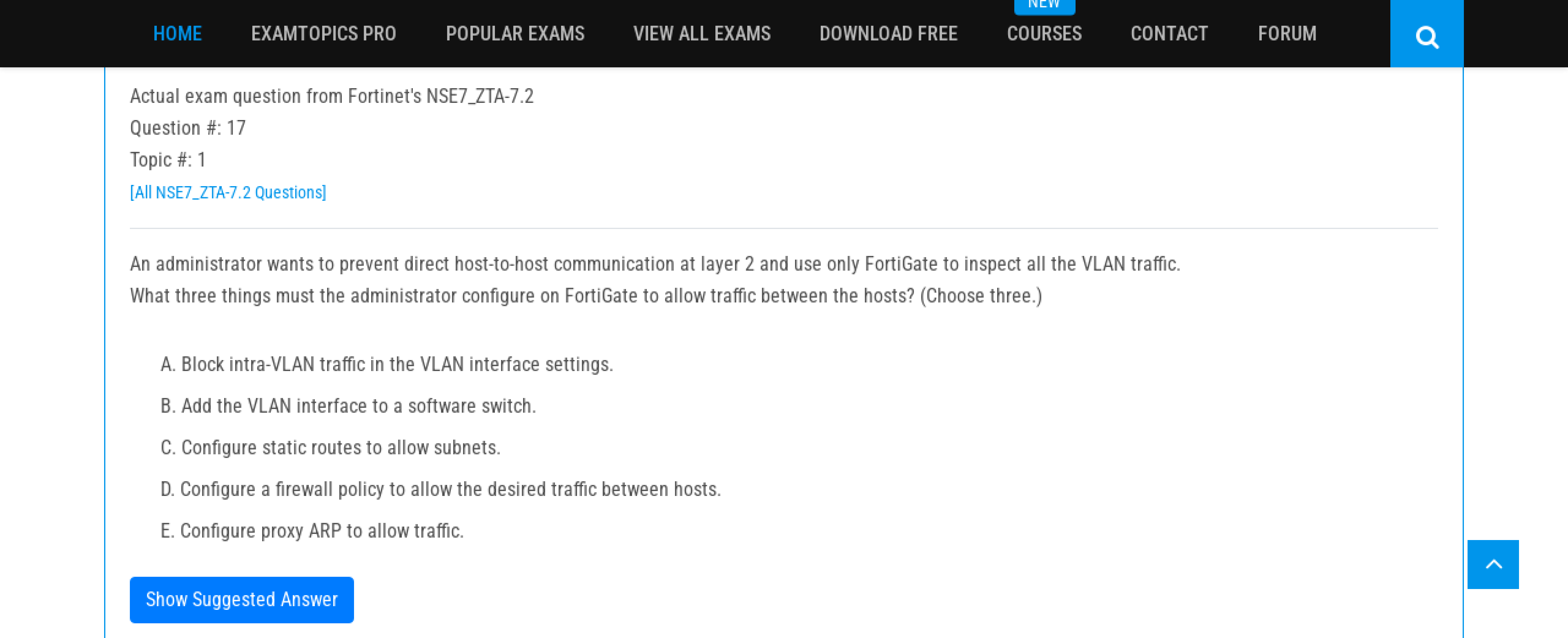
Which method is used to install passive agent on an endpoint?

A. Deployed by using a login/logout script

B. Agent is downloaded from Playstore

C. Agent is downloaded and run from captive portal

D. Installed by user or deployment tools



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 17

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

An administrator wants to prevent direct host-to-host communication at layer 2 and use only FortiGate to inspect all the VLAN traffic.

What three things must the administrator configure on FortiGate to allow traffic between the hosts? (Choose three.)

A. Block intra-VLAN traffic in the VLAN interface settings.

B. Add the VLAN interface to a software switch.

C. Configure static routes to allow subnets.

D. Configure a firewall policy to allow the desired traffic between hosts.

E. Configure proxy ARP to allow traffic.

Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 18

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

With the increase in IoT devices, which two challenges do enterprises face? (Choose two.)

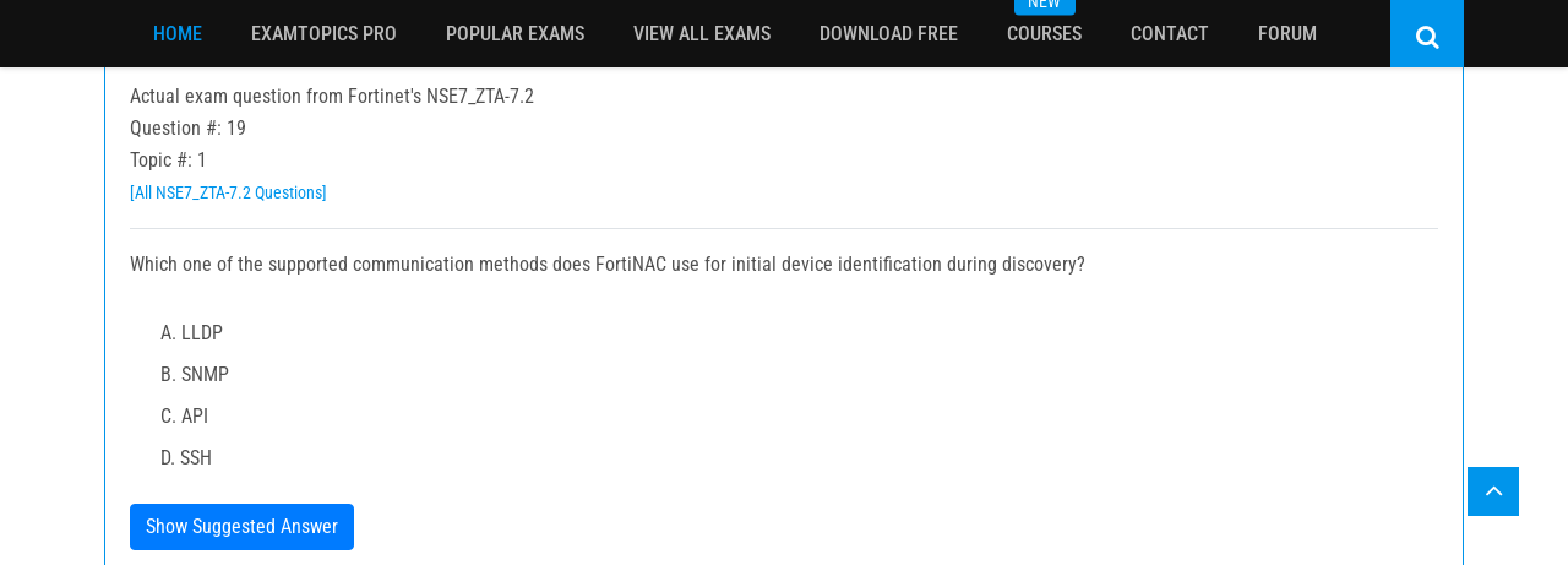
A. Bandwidth consumption due to added overhead of IoT

B. Maintaining a high performance network

C. Unpatched vulnerabilities in IoT devices

D. Achieving full network visibility

Show Suggested Answer



Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 19

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Which one of the supported communication methods does FortiNAC use for initial device identification during discovery?

A. LLDP

B. SNMP

C. API

D. SSH

Show Suggested Answer

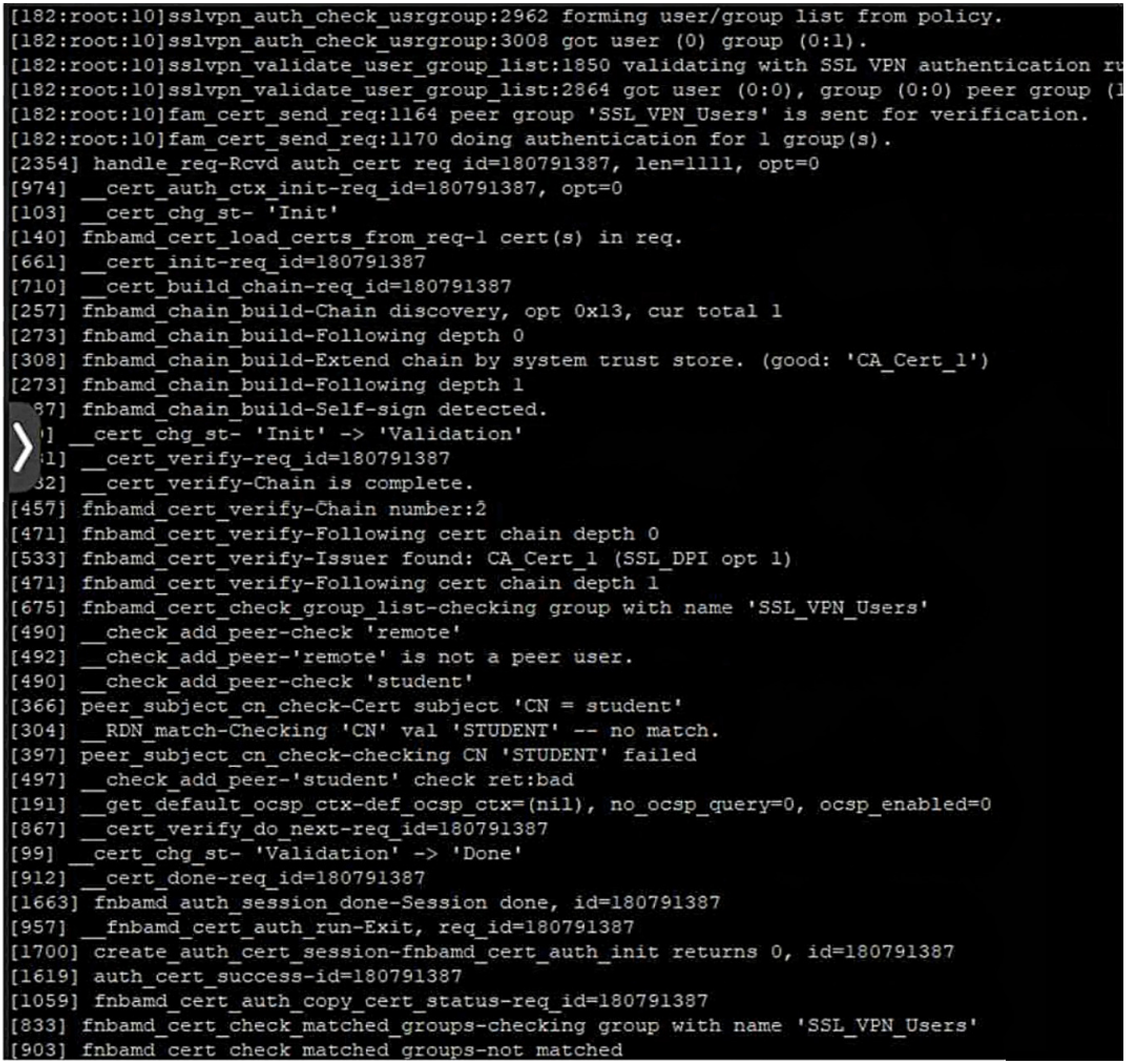
Actual exam question from Fortinet's NSE7_ZTA-7.2

Question #: 20

Topic #: 1

[All NSE7_ZTA-7.2 Questions]

Refer to the exhibit.



```
[182:root:10]sslvpn_auth_check_usrgroup:2962 forming user/group list from policy.
[182:root:10]sslvpn_auth_check_usrgroup:3008 got user (0) group (0:1).
[182:root:10]sslvpn_validate_user_group_list:1850 validating with SSL VPN authentication ru
[182:root:10]sslvpn_validate_user_group_list:2864 got user (0:0), group (0:0) peer group (1
[182:root:10]fam_cert_send_req:1164 peer group 'SSL_VPN_Users' is sent for verification.
[182:root:10]fam_cert_send_req:1170 doing authentication for 1 group(s).
[2354] handle_req-Rcvd auth_cert req id=180791387, len=1111, opt=0
[974] __cert_auth_ctx_init-req_id=180791387, opt=0
[103] __cert_chg_st- 'Init'
[140] fnbamd_cert_load_certs_from_req-1 cert(s) in req.
[661] __cert_init-req_id=180791387
[710] __cert_build_chain-req_id=180791387
[257] fnbamd_chain_build-Chain discovery, opt 0x13, cur total 1
[273] fnbamd_chain_build-Following depth 0
[308] fnbamd_chain_build-Extend chain by system trust store. (good: 'CA_Cert_1')
[273] fnbamd_chain_build-Following depth 1
 87] fnbamd_chain_build-Self-sign detected.
  ] __cert_chg_st- 'Init' -> 'Validation'
  1] __cert_verify-req_id=180791387
 32] __cert_verify-Chain is complete.
[457] fnbamd_cert_verify-Chain number:2
[471] fnbamd_cert_verify-Following cert chain depth 0
[533] fnbamd_cert_verify-Issuer found: CA_Cert_1 (SSL_DPI opt 1)
[471] fnbamd_cert_verify-Following cert chain depth 1
[675] fnbamd_cert_check_group_list-checking group with name 'SSL_VPN_Users'
[490] __check_add_peer-check 'remote'
[492] __check_add_peer-'remote' is not a peer user.
[490] __check_add_peer-check 'student'
[366] peer_subject_cn_check-Cert subject 'CN = student'
[304] __RDN_match-Checking 'CN' val 'STUDENT' -- no match.
[397] peer_subject_cn_check-checking CN 'STUDENT' failed
[497] __check_add_peer-'student' check ret:bad
[191] __get_default_ocsp_ctx-def_ocsp_ctx=(nil), no_ocsp_query=0, ocsp_enabled=0
[867] __cert_verify_do_next-req_id=180791387
[99] __cert_chg_st- 'Validation' -> 'Done'
[912] __cert_done-req_id=180791387
[1663] fnbamd_auth_session_done-Session done, id=180791387
[957] __fnbamd_cert_auth_run-Exit, req_id=180791387
[1700] create_auth_cert_session-fnbamd_cert_auth_init returns 0, id=180791387
[1619] auth_cert_success-id=180791387
[1059] fnbamd_cert_auth_copy_cert_status-req_id=180791387
[833] fnbamd_cert_check_matched_groups-checking group with name 'SSL_VPN_Users'
[903] fnbamd_cert_check_matched_groups-not matched
```

User student is not able to log in to SSL VPN.

Given the output showing a real-time debug, which statement describes the login failure?

A. Unable to verify chain of trust for the peer certificate.

B. CN does not match the user peer configuration.

C. student is not part of the usergroup SSL_VPN_Users.

D. Client certificate has expired.

Show Suggested Answer