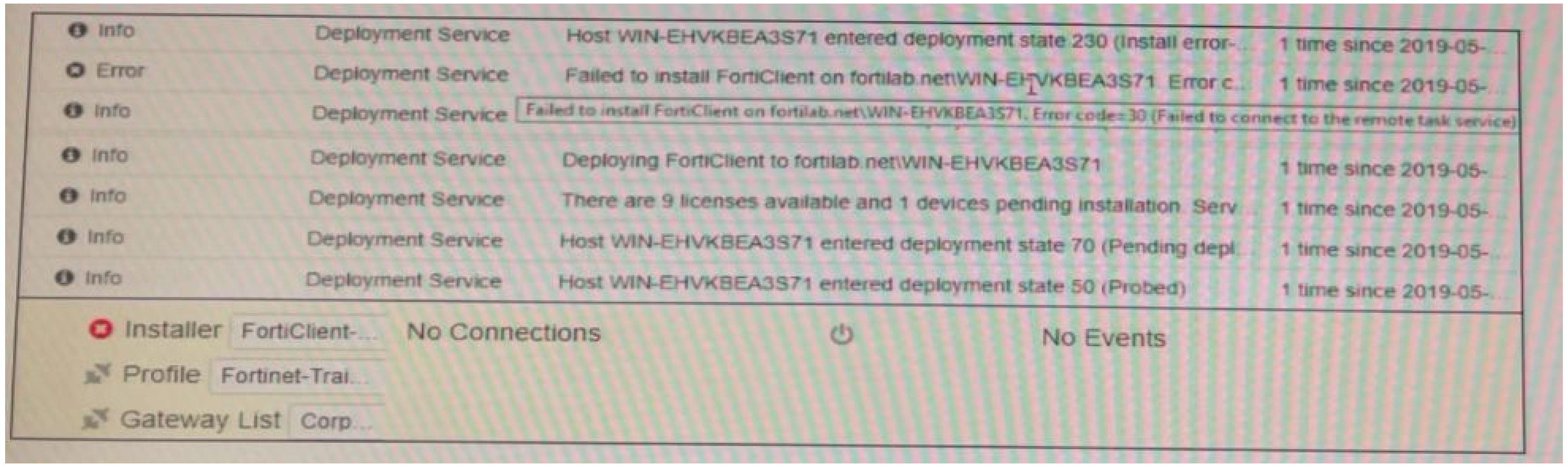
Fortinet.NSE5_FCT-7.0.by.MaryJan.27q

Number: NSE5_FCT-7.0
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: NSE5_FCT-7.0
Exam Name: Fortinet NSE 5 - FortiClient EMS 7.0

Exam A

QUESTION 1
Refer to the exhibit.



```
Info    Deployment Service   Host WIN-EHVKBEA3S71 entered deployment state 230 (Install error-...   1 time since 2019-05-...
Error   Deployment Service   Failed to install FortiClient on fortilab.net\WIN-EHVKBEA3S71. Error c...   1 time since 2019-05-...
Info    Deployment Service   Failed to install FortiClient on fortilab.net\WIN-EHVKBEA3S71. Error code=30 (Failed to connect to the remote task service)
Info    Deployment Service   Deploying FortiClient to fortilab.net\WIN-EHVKBEA3S71   1 time since 2019-05-...
Info    Deployment Service   There are 9 licenses available and 1 devices pending installation. Serv...   1 time since 2019-05-...
Info    Deployment Service   Host WIN-EHVKBEA3S71 entered deployment state 70 (Pending depl...   1 time since 2019-05-...
Info    Deployment Service   Host WIN-EHVKBEA3S71 entered deployment state 50 (Probed)   1 time since 2019-05-...

Installer     FortiClient-...   No Connections        No Events
Profile       Fortinet-Trai...
Gateway List  Corp...
```

Based on the logs shown in the exhibit, why did FortiClient EMS fail to install FortiClient on the endpoint?

A. The remote registry service is not running
B. The Windows installer service is not running
C. The task scheduler service is not running.
D. The FortiClient antivirus service is not running

Correct Answer: C
Section:
Explanation:
https://community.fortinet.com/t5/FortiClient/Technical-Note-FortiClient-fails-to-install-from-FortiClient-EMS/ta-p/193680 The deployment service error message may be caused by any of the following. Try eliminating them all, one at a time. 1. Wrong username or password in the EMS profile 2. Endpoint is unreachable over the network 3. Task Scheduler service is not running 4. Remote Registry service is not running 5. Windows firewall is blocking connection

QUESTION 2
An administrator installs FortiClient EMS in the enterprise.
Which component is responsible for enforcing protection and checking security posture?

A. FortiClient vulnerability scan
B. FortiClient EMS tags
C. FortiClient EMS
D. FortiClient

Correct Answer: D
Section:
Explanation:
FortiClient is the component that is responsible for enforcing protection and checking security posture on the endpoints. FortiClient provides features such as antivirus, web filtering, firewall, vulnerability scan, and VPN.

FortiClient EMS is the management server that centrally configures and monitors FortiClient endpoints. FortiClient EMS tags are used to group endpoints based on criteria such as OS, IP address, or domain. FortiClient vulnerability scan is a feature that detects and fixes security issues on the endpoints.Reference:=
FortiClient EMS
Compliance with EMS and FortiOS

QUESTION 3
Which three features does FortiClient endpoint security include? (Choose three.)

A. L2TP
B. IPsec
C. DLP
D. Vulnerability management
E. Real-time protection

Correct Answer: B, D, E
Section:

QUESTION 4
A new chrome book is connected in a school's network.
Which component can the EMS administrator use to manage the FortiClient web filter extension installed on the Google Chromebook endpoint?

A. FortiClient EMS
B. FortiClient site categories
C. FortiClient customer URL list
D. FortiClient web filter extension

Correct Answer: A
Section:

QUESTION 5
A FortiClient EMS administrator has enabled the compliance rule for the sales department. Which Fortinet device will enforce compliance with dynamic access control?

A. FortiClient
B. FortiClient EMS
C. FortiGate
D. FortiAnalyzer

Correct Answer: C
Section:

QUESTION 6
An administrator configures ZTNA configuration on the FortiGate for remote users. Which statement is true about the firewall policy?

A. It enforces access control
B. It redirects the client request to the access proxy
C. It defines the access proxy
D. It applies security profiles to protect traffic

Correct Answer: B
Section:
Explanation:
'The firewall policy matches and redirects client requests to the access proxy VIP' https://docs.fortinet.com/document/fortigate/7.0.0/new-features/194961/basic-ztna-configuration

QUESTION 7
An administrator wants to simplify remote access without asking users to provide user credentials.
Which access control method provides this solution'?

A. SSL VPN
B. ZTNA full mode
C. L2TP
D. ZTNA IP/MAC filtering mode

Correct Answer: B
Section:

QUESTION 8
Why does FortiGate need the root CA certificate of FortiClient EMS?

A. To sign FortiClient CSR requests
B. To revoke FortiClient client certificates
C. To trust certificates issued by FortiClient EMS
D. To update FortiClient client certificates

Correct Answer: C
Section:
Explanation:
FortiGate needs the root CA (Certificate Authority) certificate of FortiClient EMS in order to trust and validate certificates that are issued by FortiClient EMS. The root CA certificate acts as a trusted authority that verifies the authenticity and integrity of certificates issued by FortiClient EMS.

QUESTION 9
Which two statements are true about ZTNA? (Choose two.)

A. ZTNA provides role-based access
B. ZTNA manages access for remote users only
C. ZTNA manages access through the client only
D. ZTNA provides a security posture check

Correct Answer: A, D
Section:

QUESTION 10
What does FortiClient do as a fabric agent? (Choose two.)

A. Provides application inventory
B. Provides IOC verdicts

C. Automates Responses
D. Creates dynamic policies

Correct Answer: A, C
Section:

QUESTION 11
Which component or device shares ZTNA tag information through Security Fabric integration?

A. FortiClient EMS
B. FortiGate
C. FortiGate Access Proxy
D. FortiClient

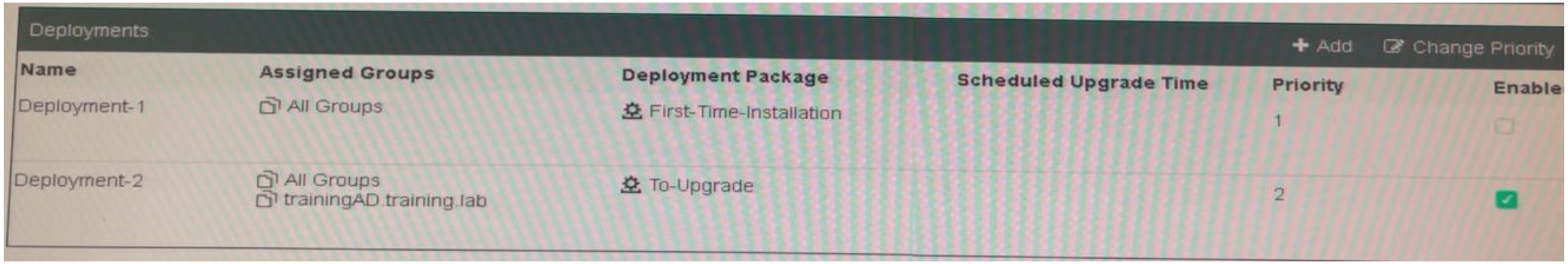
Correct Answer: A
Section:
Explanation:
FortiClient EMS is the component that shares ZTNA tag information through Security Fabric integration. ZTNA tags are synchronized from FortiClient EMS as inputs for the FortiGate application gateway. They can be used in ZTNA policies as security posture checks to ensure certain security criteria are met. FortiClient EMS can share ZTNA tags across multiple devices in the Fabric, such as FortiGate, FortiManager, and FortiAnalyzer. FortiClient EMS can also share ZTNA tags across multiple VDOMs on the same FortiGate device.FortiClient EMS can be configured to control the ZTNA tag sharing behavior in the Fabric Devices settings1.
FortiGate is the device that enforces ZTNA policies using ZTNA tags. FortiGate can receive ZTNA tags from FortiClient EMS via Fabric Connector. FortiGate can also publish ZTNA services through the ZTNA portal, which allows users to access applications without installing FortiClient.FortiGate can also provide ZTNA inline CASB for SaaS application access control2.
FortiGate Access Proxy is a feature that enables FortiGate to act as a proxy for ZTNA traffic. FortiGate Access Proxy can be deployed in front of the application servers to provide ZTNA protection. FortiGate Access Proxy can also be deployed behind the application servers to provide ZTNA visibility.FortiGate Access Proxy can use ZTNA tags to identify and authenticate users and devices2.
FortiClient is the endpoint software that connects to ZTNA services. FortiClient can register ZTNA tags with FortiClient EMS based on the endpoint security posture. FortiClient can also use ZTNA tags to access ZTNA services published by FortiGate.FortiClient can also use ZTNA tags to access SaaS applications with ZTNA inline CASB2.
Technical Tip: Behavior of ZTNA Tags shared across multiple vdoms or multiple FortiGate firewalls in the Security Fabric connected to the same FortiClient EMS Server
Synchronizing FortiClient ZTNA tags
Zero Trust Network Access (ZTNA) to Control Application Access

QUESTION 12
An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient dashboard. What must the administrator do to achieve this requirement?

A. Disable select the vulnerability scan feature in the deployment package
B. Use the default endpoint profile
C. Select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile
D. Click the hide icon on the vulnerability scan tab

Correct Answer: D
Section:

QUESTION 13
Refer to the exhibit.



Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enable
Deployment-1	All Groups	First-Time-Installation		1	☐
Deployment-2	All Groups trainingAD.training.lab	To-Upgrade		2	☑

Which shows FortiClient EMS deployment profiles.
When an administrator creates a deployment profile on FortiClient EMS, which statement about the deployment profile is true?

A. Deployment-1 will install FortiClient on new AD group endpoints
B. Deployment-2 will install FortiClient on both the AD group and workgroup
C. Deployment-2 will upgrade FortiClient on both the AD group and workgroup
D. Deployment-1 will upgrade FortiClient only on the workgroup

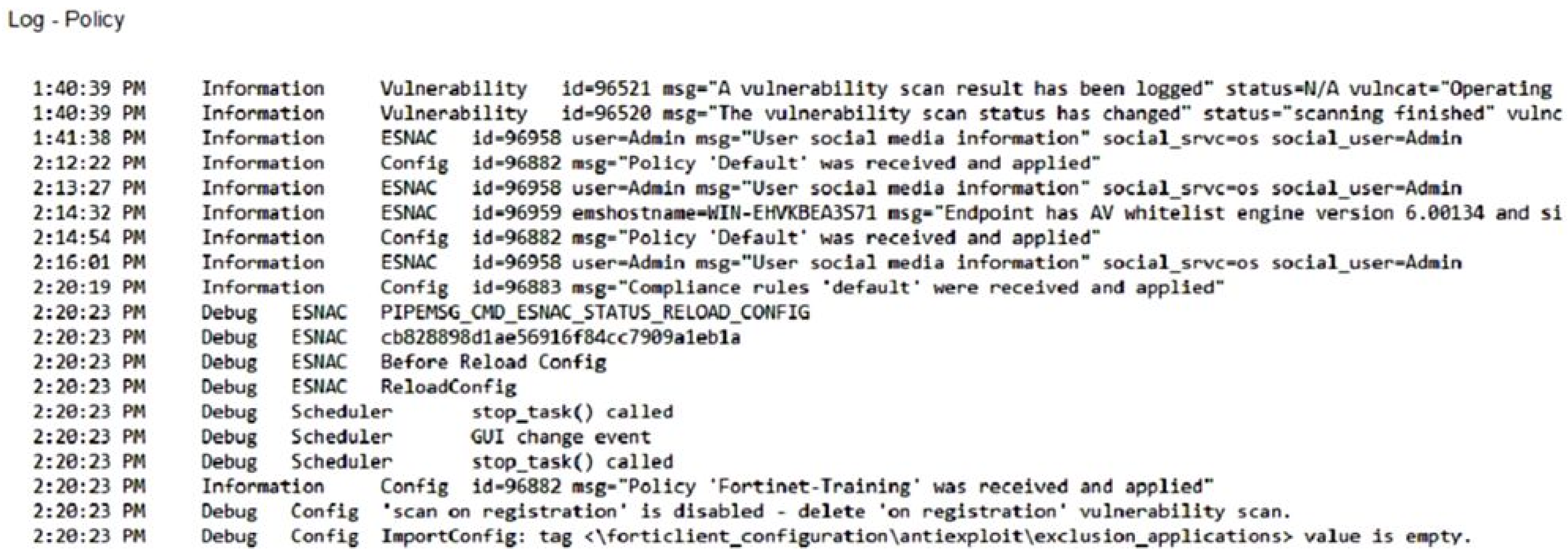
Correct Answer: C
Section:

QUESTION 14
An administrator needs to connect FortiClient EMS as a fabric connector to FortiGate. What is the prerequisite to get FortiClient EMS to connect to FortiGate successfully?

A. Revoke and update the FortiClient EMS root CA.
B. Revoke and update the FortiClient client certificate on EMS.
C. Import and verify the FortiClient client certificate on FortiGate.
D. Import and verify the FortiClient EMS root CA certificate on FortiGate

Correct Answer: D
Section:
Explanation:
The FortiClient EMS root CA certificate needs to be imported and verified on the FortiGate appliance. This allows the FortiGate to trust the certificate authority (CA) used by FortiClient EMS for issuing client certificates. By importing and verifying the root CA certificate, FortiGate can establish a secure connection with FortiClient EMS and validate the authenticity of the client certificates presented during the connection process.

QUESTION 15
Refer to the exhibit.



Log - Policy

```
  1:40:39 PM     Information     Vulnerability   id=96521 msg="A vulnerability scan result has been logged" status=N/A vulncat="Operating
  1:40:39 PM     Information     Vulnerability   id=96520 msg="The vulnerability scan status has changed" status="scanning finished" vulnc
  1:41:38 PM     Information     ESNAC   id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
  2:12:22 PM     Information     Config  id=96882 msg="Policy 'Default' was received and applied"
  2:13:27 PM     Information     ESNAC   id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
  2:14:32 PM     Information     ESNAC   id=96959 emshostname=WIN-EHVKBEA3S71 msg="Endpoint has AV whitelist engine version 6.00134 and si
  2:14:54 PM     Information     Config  id=96882 msg="Policy 'Default' was received and applied"
  2:16:01 PM     Information     ESNAC   id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
  2:20:19 PM     Information     Config  id=96883 msg="Compliance rules 'default' were received and applied"
  2:20:23 PM     Debug   ESNAC   PIPEMSG_CMD_ESNAC_STATUS_RELOAD_CONFIG
  2:20:23 PM     Debug   ESNAC   cb828898d1ae56916f84cc7909a1eb1a
  2:20:23 PM     Debug   ESNAC   Before Reload Config
  2:20:23 PM     Debug   ESNAC   ReloadConfig
  2:20:23 PM     Debug   Scheduler       stop_task() called
  2:20:23 PM     Debug   Scheduler       GUI change event
  2:20:23 PM     Debug   Scheduler       stop_task() called
  2:20:23 PM     Information     Config  id=96882 msg="Policy 'Fortinet-Training' was received and applied"
  2:20:23 PM     Debug   Config  'scan on registration' is disabled - delete 'on registration' vulnerability scan.
  2:20:23 PM     Debug   Config  ImportConfig: tag <\forticlient_configuration\antiexploit\exclusion_applications> value is empty.
```

Based on the FortiClient logs shown in the exhibit which endpoint profile policy is currently applied to the FortiClient endpoint from the EMS server?

A. Default

B. Compliance rules default

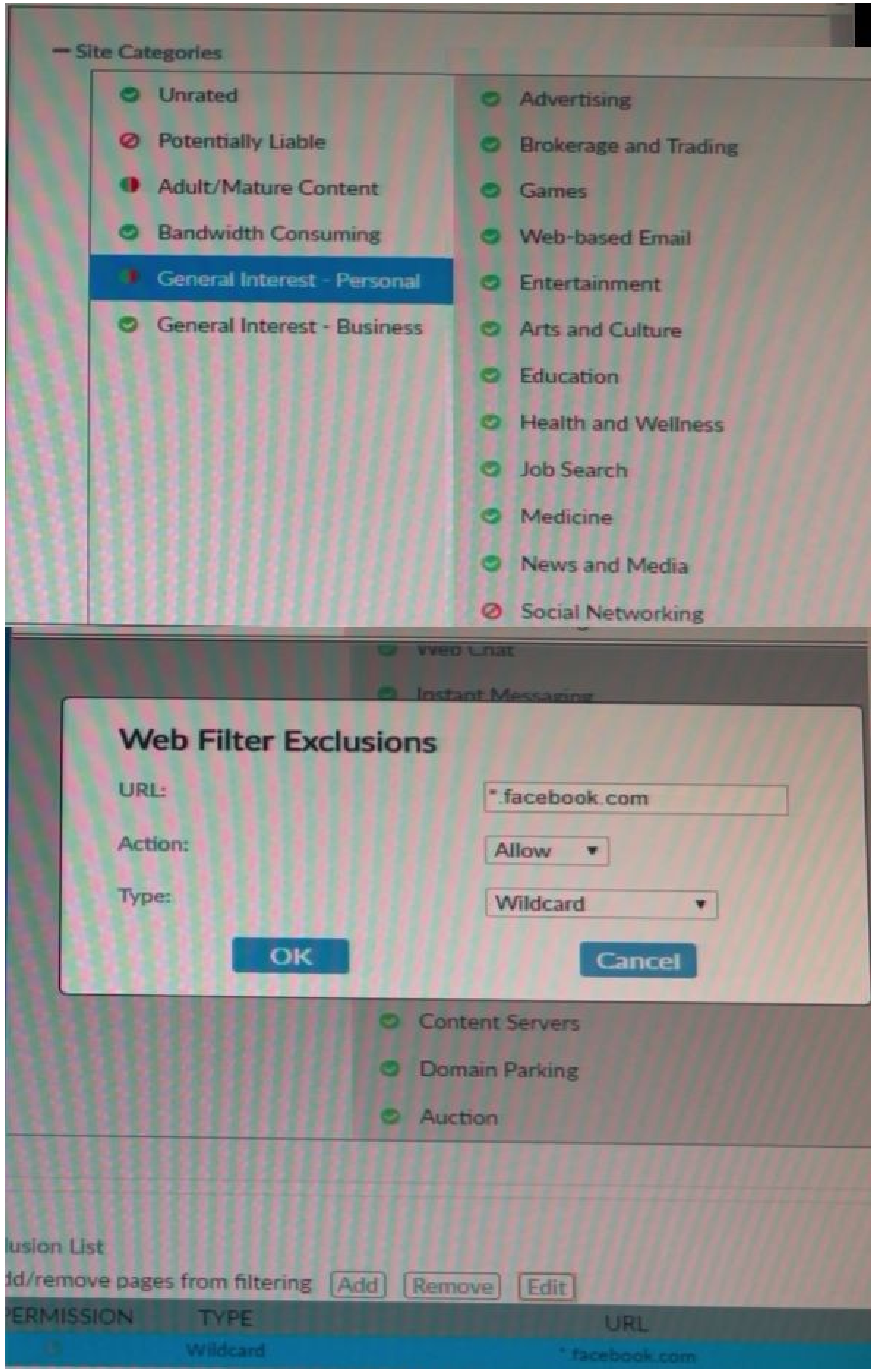
C. Fortinet- Training

D. Default configuration policy

Correct Answer: C
Section:

QUESTION 16

Refer to the exhibit.



— Site Categories

- ✓ Unrated
- ⊘ Potentially Liable
- ◐ Adult/Mature Content
- ✓ Bandwidth Consuming
- ◐ General Interest - Personal
- ✓ General Interest - Business
- ✓ Advertising
- ✓ Brokerage and Trading
- ✓ Games
- ✓ Web-based Email
- ✓ Entertainment
- ✓ Arts and Culture
- ✓ Education
- ✓ Health and Wellness
- ✓ Job Search
- ✓ Medicine
- ✓ News and Media
- ⊘ Social Networking
- ✓ Web Chat
- ✓ Instant Messaging
- ✓ Content Servers
- ✓ Domain Parking
- ✓ Auction

Web Filter Exclusions

URL: *.facebook.com

Action: Allow ▾

Type: Wildcard ▾

lusion List

dd/remove pages from filtering

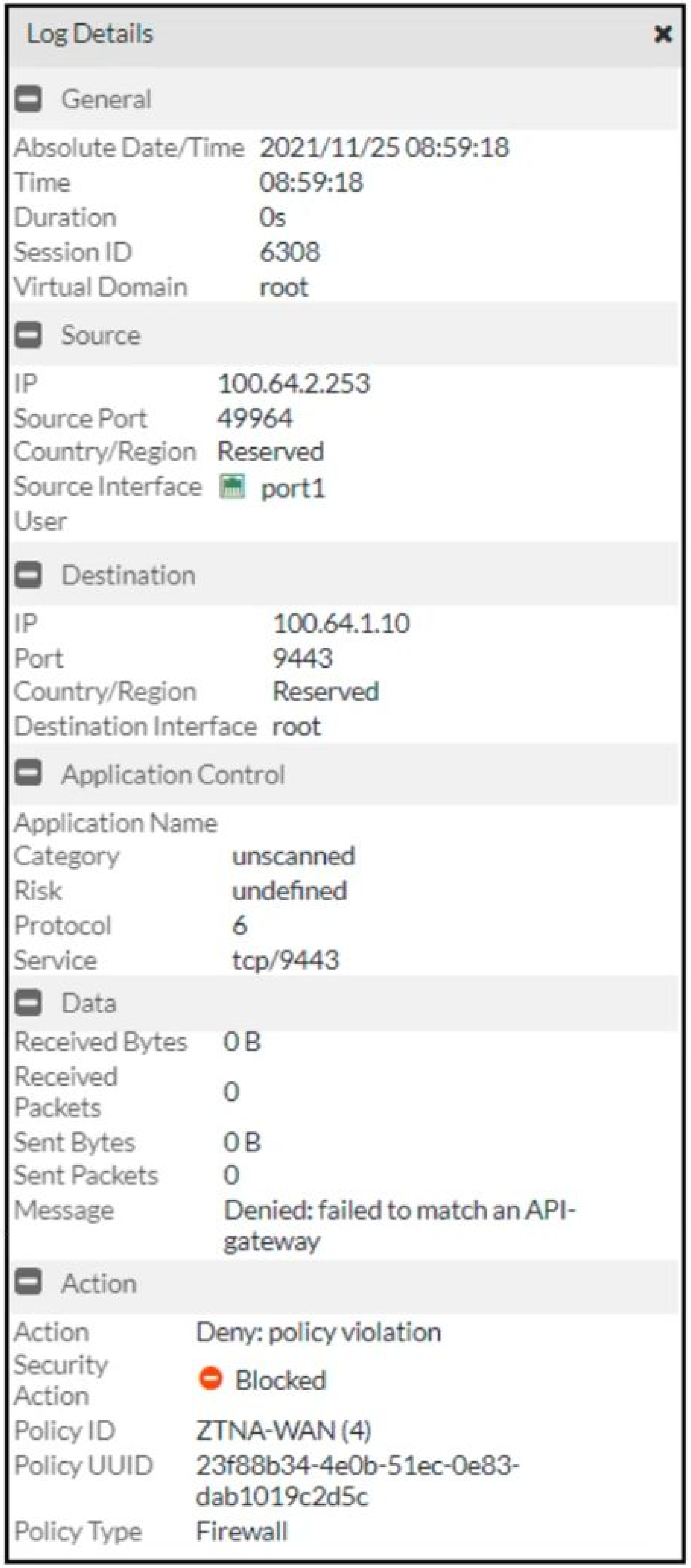
ERMISSION	TYPE	URL
✓	Wildcard	*.facebook.com

<a target='_blank' href='http://www.facebook.com/'>Based on the settings shown in the exhibit, which action will FortiClient take when users try to access www.facebook.com?</a>

A. FortiClient will allow access to Facebook
B. FortiClient will monitor only the user's web access to the Facebook website
C. FortiClient will block access to Facebook and its subdomains.
D. FortiClient will prompt a warning message to warn the user before they can access the Facebook website

Correct Answer: A
Section:

QUESTION 17
Refer to the exhibit.



Log Details

General

Absolute Date/Time	2021/11/25 08:59:18
Time	08:59:18
Duration	0s
Session ID	6308
Virtual Domain	root

Source

IP	100.64.2.253
Source Port	49964
Country/Region	Reserved
Source Interface	port1
User	

Destination

IP	100.64.1.10
Port	9443
Country/Region	Reserved
Destination Interface	root

Application Control

Application Name	
Category	unscanned
Risk	undefined
Protocol	6
Service	tcp/9443

Data

Received Bytes	0 B
Received Packets	0
Sent Bytes	0 B
Sent Packets	0
Message	Denied: failed to match an API-gateway

Action

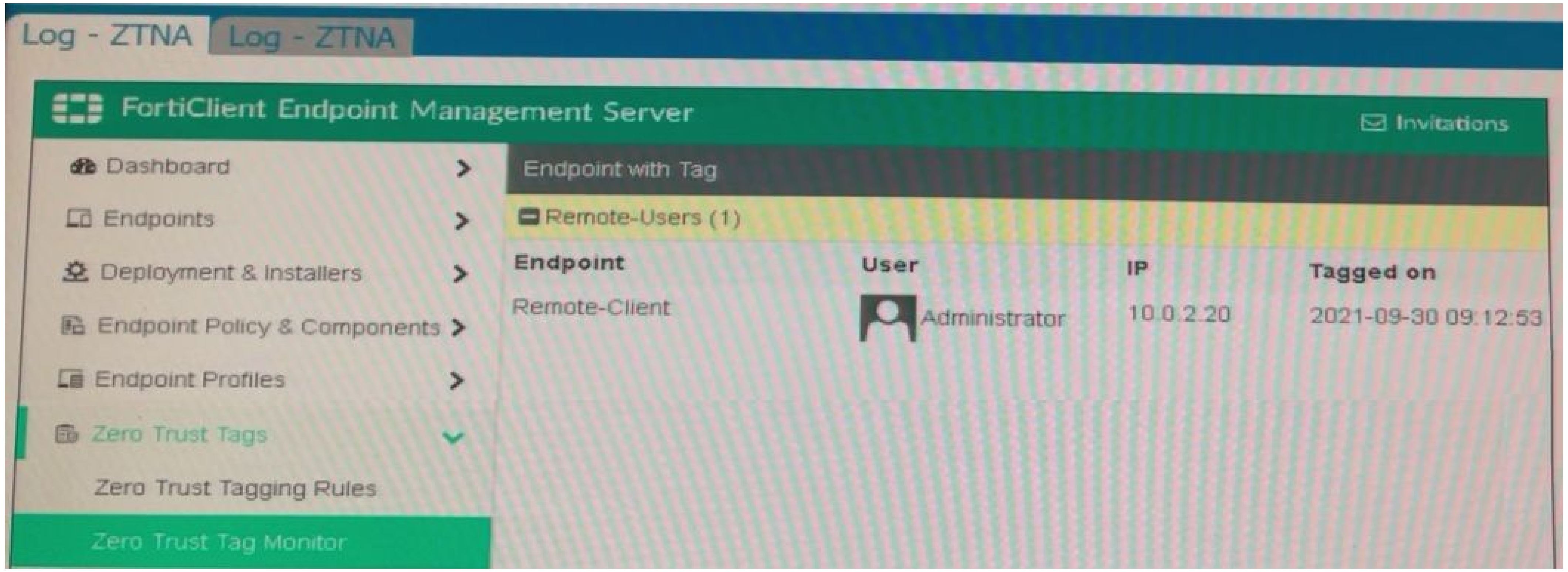
Action	Deny: policy violation
Security Action	Blocked
Policy ID	ZTNA-WAN (4)
Policy UUID	23f88b34-4e0b-51ec-0e83-dab1019c2d5c
Policy Type	Firewall

Which shows the output of the ZTNA traffic log on FortiGate.
What can you conclude from the log message?

A. The remote user connection does not match the explicit proxy policy.
B. The remote user connection does not match the ZTNA server configuration.
C. The remote user connection does not match the ZTNA rule configuration.
D. The remote user connection does not match the ZTNA firewall policy

Correct Answer: C
Section:

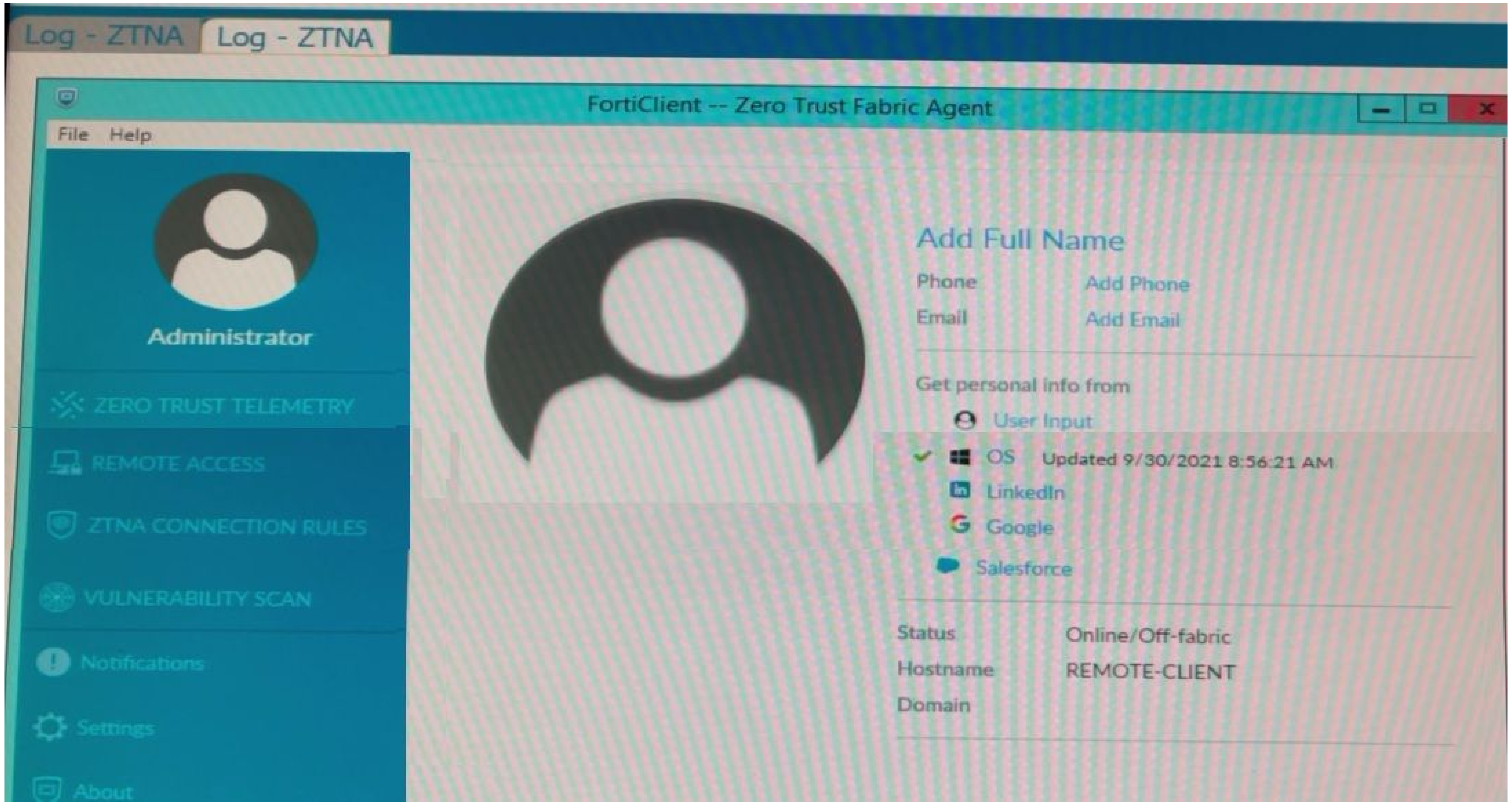
QUESTION 18
Refer to the exhibits.



Endpoint with Tag

Remote-Users (1)

Endpoint	User	IP	Tagged on
Remote-Client	Administrator	10.0.2.20	2021-09-30 09:12:53



Add Full Name

Phone Add Phone

Email Add Email

Get personal info from

- User Input
- ✓ OS Updated 9/30/2021 8:56:21 AM
- LinkedIn
- Google
- Salesforce

Status Online/Off-fabric

Hostname REMOTE-CLIENT

Domain

Which show the Zero Trust Tag Monitor and the FortiClient GUI status.
Remote-Client is tagged as Remote-Users on the FortiClient EMS Zero Trust Tag Monitor.
What must an administrator do to show the tag on the FortiClient GUI?

A. Update tagging rule logic to enable tag visibility
B. Change the FortiClient system settings to enable tag visibility
C. Change the endpoint control setting to enable tag visibility
D. Change the user identity settings to enable tag visibility

Correct Answer: B
Section:

QUESTION 19
Which two third-party tools can an administrator use to deploy FortiClient? (Choose two.)

A. Microsoft Windows Installer
B. Microsoft SCCM
C. Microsoft Active Directory GPO
D. QR code generator

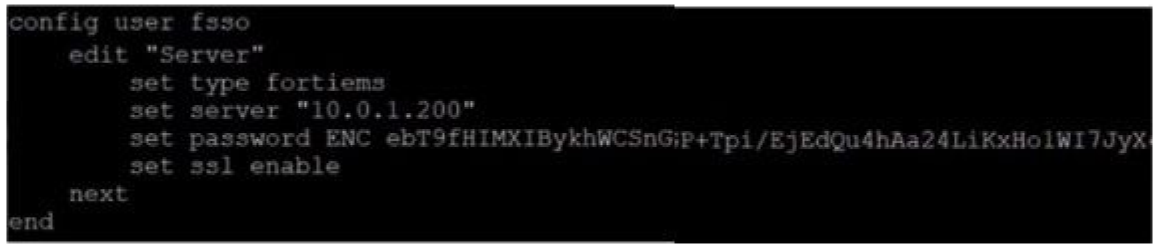
Correct Answer: B, C
Section:

QUESTION 20
Which two statements are true about the ZTNA rule? (Choose two.)

A. It enforces access control
B. It redirects the client request to the access proxy
C. It defines the access proxy
D. It applies security profiles to protect traffic

Correct Answer: A, D
Section:
Explanation:
'A ZTNA rule is a proxy policy used to enforce access control. ZTNA tags or tag groups can be defined to enforce zero trust role based access. Security profiles can be configured to protect this traffic.'
'ZTNA rules help control access by defining users and ZTNA tags to perform user authentication and security posture checks. And just like firewall policies, you can control the source and destination addresses, and apply appropriate security profiles to scan the traffic.' https://docs.fortinet.com/document/fortigate/7.0.0/ztna-deployment/899992/configuring-ztna-rules-to-control-access

QUESTION 21
Refer to the exhibit.



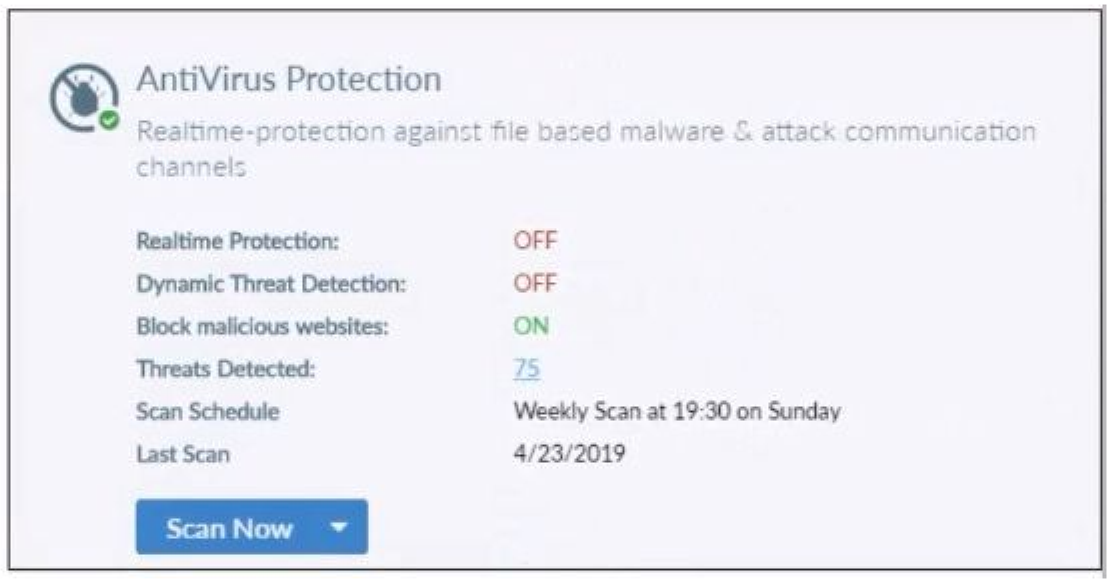
```
config user fsso
    edit "Server"
        set type fortiems
        set server "10.0.1.200"
        set password ENC ebT9fHIMXIBykhWCSnG;P+Tpi/EjEdQu4hAa24LiKxHo1WI7JyX
        set ssl enable
    next
end
```

Based on the CLI output from FortiGate. which statement is true?

A. FortiGate is configured to pull user groups from FortiClient EMS
B. FortiGate is configured with local user group
C. FortiGate is configured to pull user groups from FortiAuthenticator
D. FortiGate is configured to pull user groups from AD Server.

Correct Answer: A
Section:

QUESTION 22
Refer to the exhibit.



AntiVirus Protection

Realtime-protection against file based malware & attack communication channels

Realtime Protection: OFF

Dynamic Threat Detection: OFF

Block malicious websites: ON

Threats Detected: 75

Scan Schedule: Weekly Scan at 19:30 on Sunday

Last Scan: 4/23/2019

Based on the settings shown in the exhibit what action will FortiClient take when it detects that a user is trying to download an infected file?

A. Blocks the infected files as it is downloading
B. Quarantines the infected files and logs all access attempts
C. Sends the infected file to FortiGuard for analysis
D. Allows the infected file to download without scan

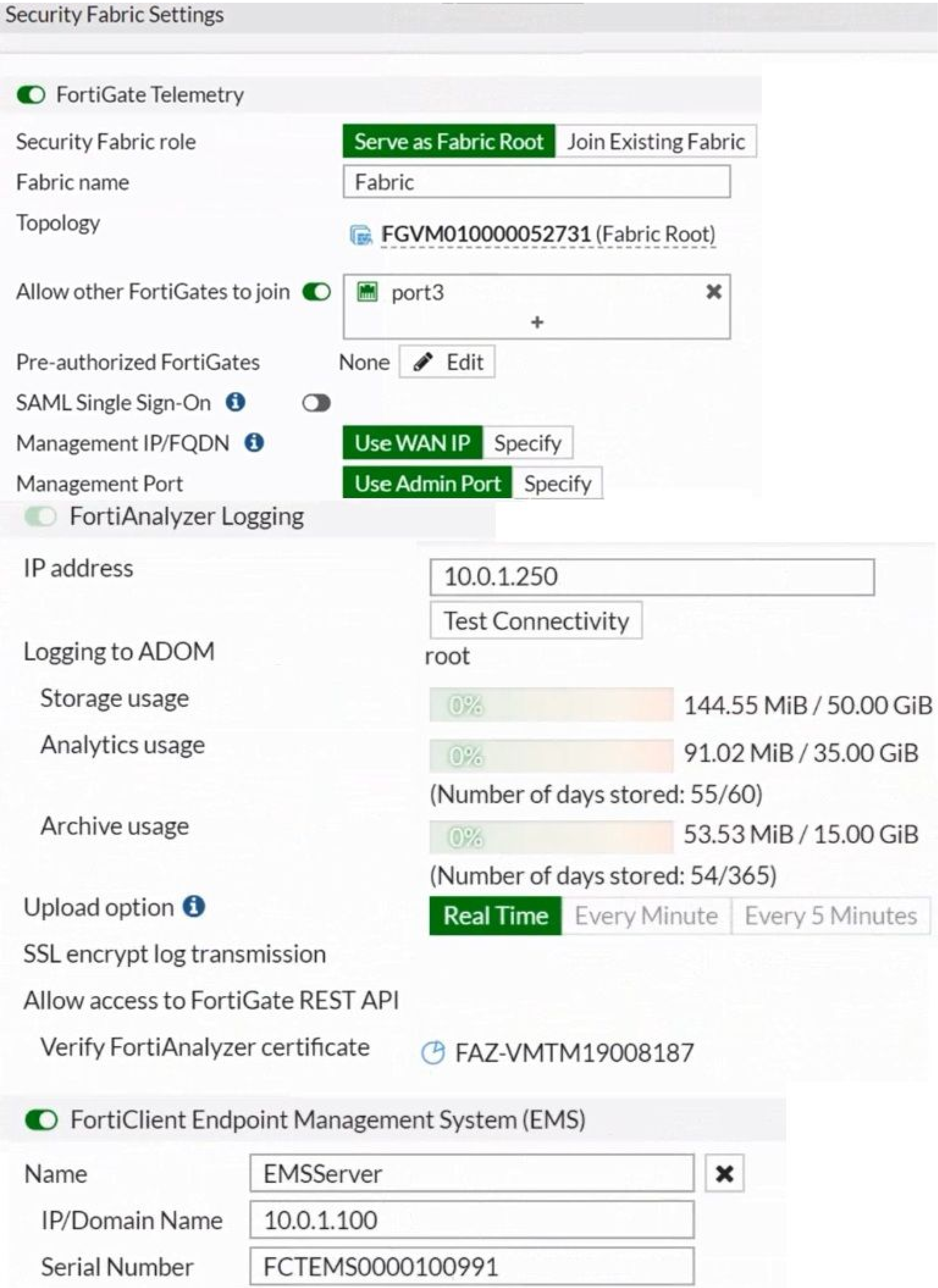
Correct Answer: D
Section:
Explanation:
Block Malicious Website has nothing to do with infected files. Since Realtime Protection is OFF, it will be allowed without being scanned.

QUESTION 23
An administrator deploys a FortiClient installation through the Microsoft AD group policy After installation is complete all the custom configuration is missing.
What could have caused this problem?

A. The FortiClient exe file is included in the distribution package
B. The FortiClient MST file is missing from the distribution package
C. FortiClient does not have permission to access the distribution package.
D. The FortiClient package is not assigned to the group

Correct Answer: D
Section:

QUESTION 24
Refer to the exhibits.



Security Fabric Settings

● FortiGate Telemetry

Security Fabric role: [✓ Serve as Fabric Root] Join Existing Fabric

Fabric name: Fabric

Topology: FGVM010000052731 (Fabric Root)

Allow other FortiGates to join ●: port3 ✖ +

Pre-authorized FortiGates: None Edit

SAML Single Sign-On ℹ ○

Management IP/FQDN ℹ: [✓ Use WAN IP] Specify

Management Port: [✓ Use Admin Port] Specify

● FortiAnalyzer Logging

IP address: 10.0.1.250

Test Connectivity

Logging to ADOM: root

Storage usage: 0% 144.55 MiB / 50.00 GiB

Analytics usage: 0% 91.02 MiB / 35.00 GiB
(Number of days stored: 55/60)

Archive usage: 0% 53.53 MiB / 15.00 GiB
(Number of days stored: 54/365)

Upload option ℹ: [✓ Real Time] Every Minute Every 5 Minutes

SSL encrypt log transmission

Allow access to FortiGate REST API

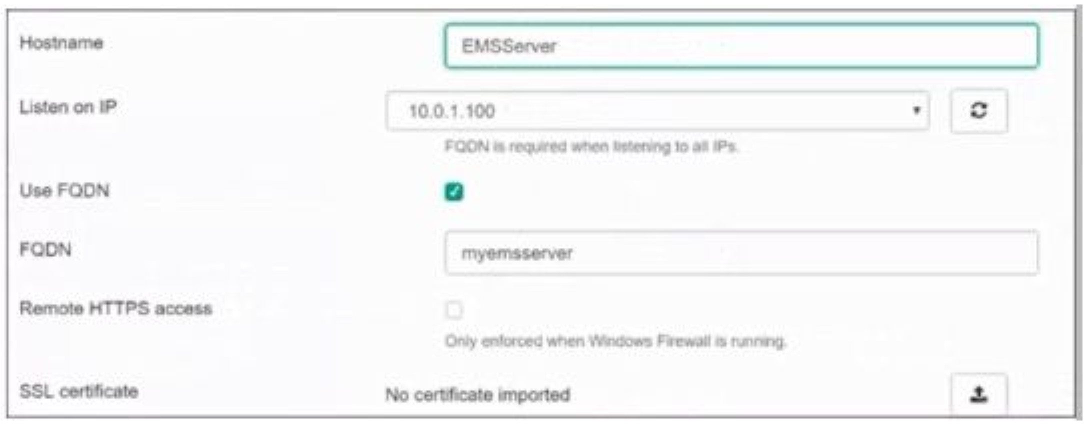
Verify FortiAnalyzer certificate: FAZ-VMTM19008187

● FortiClient Endpoint Management System (EMS)

Name: EMSServer ✖

IP/Domain Name: 10.0.1.100

Serial Number: FCTEMS0000100991



Hostname	EMSServer
Listen on IP	10.0.1.100 FQDN is required when listening to all IPs.
Use FQDN	☑
FQDN	myemsserver
Remote HTTPS access	□ Only enforced when Windows Firewall is running.
SSL certificate	No certificate imported

Based on the FortiGate Security Fabric settings shown in the exhibits, what must an administrator do on the EMS server to successfully quarantine an endpoint. when it is detected as a compromised host (loC)?

A. The administrator must enable remote HTTPS access to EMS.
B. The administrator must enable FQDN on EMS.
C. The administrator must authorize FortiGate on FortiAnalyzer.
D. The administrator must enable SSH access to EMS.

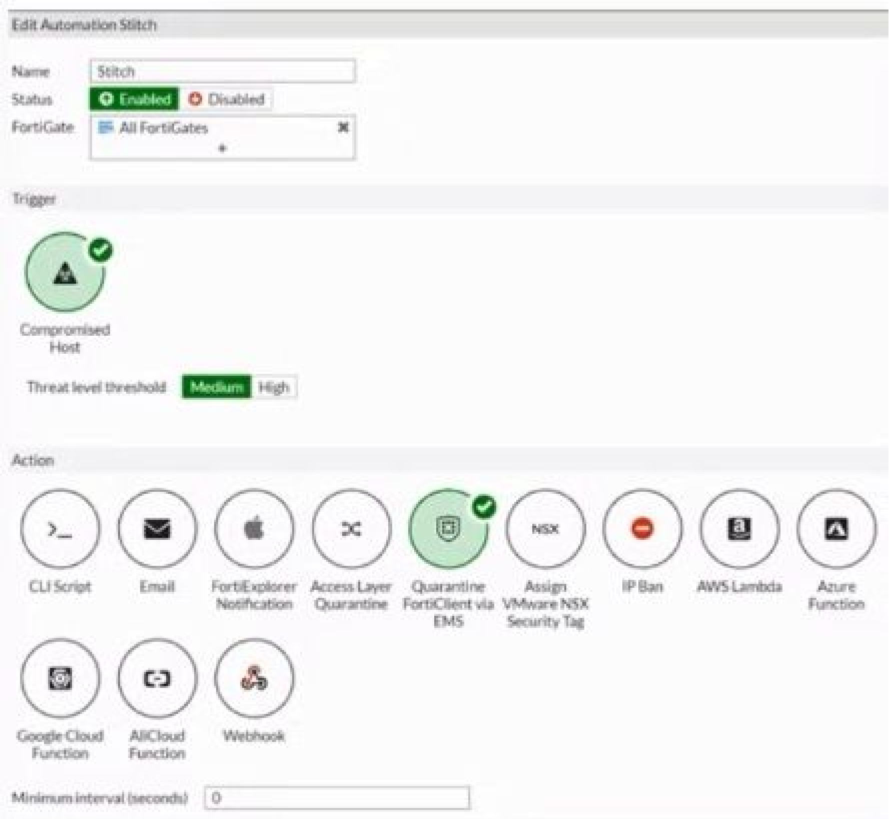
Correct Answer: A
Section:

QUESTION 25
Which statement about FortiClient comprehensive endpoint protection is true?

A. It helps to safeguard systems from email spam
B. It helps to safeguard systems from data loss.
C. It helps to safeguard systems from DDoS.
D. lt helps to safeguard systems from advanced security threats, such as malware.

Correct Answer: D
Section:
Explanation:
FortiClient provides comprehensive endpoint protection for your Windows-based, Mac-based, and Linuxbased desktops, laptops, file servers, and mobile devices such as iOS and Android. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

QUESTION 26
Refer to the exhibit.



Edit Automation Stitch

Name: Stitch

Status: [✓ Enabled] Disabled

FortiGate: All FortiGates

Trigger

Compromised Host ✓

Threat level threshold: [✓ Medium] High

Action

Quarantine FortiClient via EMS ✓

Minimum interval (seconds): 0

Based on the Security Fabric automation settings, what action will be taken on compromised endpoints?

A. Endpoints will be quarantined through EMS
B. Endpoints will be banned on FortiGate
C. An email notification will be sent for compromised endpoints
D. Endpoints will be quarantined through FortiSwitch

Correct Answer: A
Section:

QUESTION 27
In a FortiSandbox integration, what does the remediation option do?

A. Wait for FortiSandbox results before allowing files
B. Exclude specified files
C. Alert and notify only
D. Deny access to a file when it sees no results

Correct Answer: C
Section:
Explanation:
Under 'Remediation Options' section, there are only two options (Quarantine infected files, Alert & Notify only). https://docs.fortinet.com/document/forticlient/6.0.0/administration-guide/657996/configuring-submission-access-and-remediation#:~:text=disable%20this%20feature.-,Remediation%20Options,-Quarantine%20infected%20files