

Fortinet

Exam Questions FCP_FCT_AD-7.2

FCP-FortiClient EMS 7.2 Administrator



NEW QUESTION 1

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

Answer: D

Explanation:

For managing the FortiClient web filter extension installed on the Google Chromebook endpoint, the EMS administrator can use the following component:

? FortiClient EMS (Enterprise Management Server) is designed to manage and control multiple FortiClient installations across various endpoints.

? EMS provides centralized management for endpoint policies, including web filtering configurations.

? The EMS administrator can configure and enforce web filter policies on Chromebooks through the EMS console.

Therefore, FortiClient EMS is the correct component for managing the web filter extension on Google Chromebook endpoints.

References

? FortiClient EMS 7.2 Study Guide, Chromebook Management Section

? Fortinet Documentation on FortiClient EMS and Web Filtering for Chromebooks

NEW QUESTION 2

An administrator has a requirement to add user authentication to the ZTNA access for remote or off-fabric users. Which FortiGate feature is required in addition to ZTNA?

- A. FortiGate FSSO
- B. FortiGate certificates
- C. FortiGate explicit proxy
- D. FortiGate endpoint control

Answer: C

Explanation:

For adding user authentication to the ZTNA access for remote or off-fabric users, the following FortiGate feature is required in addition to ZTNA:

? FortiGate explicit proxy allows FortiGate to intercept web traffic for authentication purposes.

? ZTNA integrates with various FortiGate features to provide secure access and ensure that users are authenticated before accessing resources.

? By using an explicit proxy, FortiGate can handle web traffic and enforce authentication policies for remote users who are not directly on the corporate network (off-fabric).

Thus, the correct feature to use for this requirement is the FortiGate explicit proxy.

References

? FortiGate Security 7.2 Study Guide, ZTNA and Proxy Configuration Sections

? Fortinet Documentation on FortiGate Explicit Proxy and ZTNA Integration

NEW QUESTION 3

Refer to the exhibit.

Log - File

Filename

Unconfirmed 899290.crdownload

Original Location

\\??\C:\Users

Date Quarantined

Submitted

Not Submitted

Status

Quarantined

Virus Name

EICAR_TEST_FILE

Quarantined File Name

QuarantFile2cf63303_2172

Log File Location

Quarantined By

Realtime Protection

Close

Based on the FortiClient tog details shown in the exhibit, which two statements ace true? (Choose two.)

- A. The filename Is Unconfirmed 899290.crdovnload.
- B. The file status is Quarantined
- C. The filename is sent to FortiSandbox for further inspection.
- D. The file location is \\??\D:\Users\.

Answer: AB

NEW QUESTION 4

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

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

Answer: C

Explanation:

? Requirement Analysis:

? Evaluating Options:
? Conclusion:
References:
? FortiClient EMS feature configuration and management documentation from the study guides.

NEW QUESTION 5

When site categories are disabled in FortiClient web filter, which feature can be used to protect the endpoint from malicious web access?

- A. Real-time protection list
- B. Block malicious websites on antivirus
- C. FortiSandbox URL list
- D. Web exclusion list

Answer: D

Explanation:

? Web Filter Functionality:
? Alternative Protection Features:
? Conclusion:
References:
? FortiClient web filter configuration and features from the study guides.

NEW QUESTION 6

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

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

Answer: C

Explanation:

? Understanding FortiClient EMS Components:
? Evaluating Responsibilities:
? Conclusion:
References:
? FortiClient EMS and endpoint security documentation from the study guides.

NEW QUESTION 7

Exhibit.

Zero Trust Tag Monitor

FortiClient Endpoint Management Server

Dashboard > Endpoints > Deployment & Installers > Endpoint Policy & Components > Endpoint Profiles > **Zero Trust Tags** > Zero Trust Tagging Rules > **Zero Trust Tag Monitor** > FortiGuard Outbreak Detections >

Endpoint with Tag

Compliant (2)

Low (2)

Remote-Endpoints (1)

Endpoint	User	OS	IP
Remote-Client	Administrator	Microsoft Windows S...	10.0.2.20

Showing: 1 Total: 1

FortiClient Status - GUI

FortiClient -- Zero Trust Fabric Agent

File Help

Administrator

ZERO TRUST TELEMTRY

REMOTE ACCESS

MALWARE PROTECTION

WEB FILTER

VULNERABILITY SCAN

Add Full Name

Phone Add Phone

Email Add Email

Get personal info from

User Input

OS Updated 6/21/2023 1:32:55 PM

LinkedIn

Google

Salesforce

Status Online/Off-fabric

Hostname REMOTE-CLIENT

Activate Windows

Refer to the exhibits, which show the Zero Trust Tag Monitor and the FortiClient GUI status.

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

- A. Change the FortiClient EMS shared settings to enable tag visibility.
- B. Change the endpoint alerts configuration to enable tag visibility.
- C. Update tagging rule logic to enable tag visibility.
- D. Change the FortiClient system settings to enable tag visibility.

Answer: B

Explanation:

? Observation of Exhibits:

? Enabling Tag Visibility:

? Verification:

References:

? FortiClient EMS and FortiClient configuration documentation from the study guides.

NEW QUESTION 8

Which statement about FortiClient enterprise management server is true?

- A. It provides centralized management of FortiGate devices.
- B. It provides centralized management of multiple endpoints running FortiClient software.
- C. It provides centralized management of FortiClient Android endpoints only.
- D. It provides centralized management of Chromebooks running real-time protection

Answer: B

Explanation:

FortiClient EMS is designed to provide centralized management and control of multiple endpoints running FortiClient software. It serves as a central management server that allows administrators to efficiently manage and configure a large number of FortiClient installations across the network.

NEW QUESTION 9

Which component or device shares device status information through ZTNA telemetry?

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

Answer: A

Explanation:

FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry.

NEW QUESTION 10

Exhibit.

```
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-EHVKB8EA3S71 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 cb828898d1ae56916f84cc7909a1ebla
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. Fortinet-Training
- B. Default configuration policy c
- C. Compliance rules default
- D. Default

Answer: A

Explanation:

? Observation of Logs:

? Evaluating Policies:

? Conclusion:

References:

? FortiClient EMS policy configuration and log analysis documentation from the study guides.

NEW QUESTION 10

An administrator installs FortiClient on Windows Server. What is the default behavior of real-time protection control?

- A. Real-time protection must update AV signature database
- B. Real-time protection sends malicious files to FortiSandbox when the file is not detected locally
- C. Real-time protection is disabled
- D. Real-time protection must update the signature database from FortiSandbox

Answer: C

Explanation:

When FortiClient is installed on a Windows Server, the default behavior for real-time protection control is:

? Real-time protection is disabled:By default, FortiClient does not enable real-time

protection on server installations to avoid potential performance impacts and because servers typically have different security requirements compared to client endpoints.

Thus, real-time protection is disabled by default on Windows Server installations.

References

? FortiClient EMS 7.2 Study Guide, Real-time Protection Section

? Fortinet Documentation on FortiClient Default Settings for Server Installations

NEW QUESTION 11

Refer to the exhibit, which shows the Zero Trust Tagging Rule Set configuration.

Zero Trust Tagging Rule Set

Name

Compliance

Tag Endpoint As ⓘ

Compliant

Enabled

Comments

Optional

Rules

↺ Default Logic + Add Rule

Type	Value
Windows (2)	
AntiVirus Software	1 AV Software is installed and running
OS Version	2 Windows Server 2012 R2
	3 Windows 10

Rule Logic ⓘ

(1 and 3) or 2

↺ Reset

Which two statements about the rule set are true? (Choose two.)

- A. The endpoint must satisfy that only Windows 10 is running.
- B. The endpoint must satisfy that only AV software is installed and running.
- C. The endpoint must satisfy that antivirus is installed and running and Windows 10 is running.
- D. The endpoint must satisfy that only Windows Server 2012 R2 is running.

Answer: CD

Explanation:

Based on the Zero Trust Tagging Rule Set configuration shown in the exhibit:

- ? The rule set includes two conditions:
- ? The Rule Logic is specified as "(1 and 3) or 2," meaning: Therefore, the endpoint must satisfy either:
- ? Antivirus is installed and running and Windows 10 is running.
- ? Windows Server 2012 R2 is running.

References

- ? FortiClient EMS 7.2 Study Guide, Zero Trust Tagging Rule Set Configuration Section
- ? Fortinet Documentation on Configuring Zero Trust Tagging Rules and Logic

NEW QUESTION 13

Refer to the exhibit.

```
config user fsso
  edit "Server"
    set type fortiems
    set server "10.0.1.200"
    set password ENC ebT9fHIMXIBykhWCSnG;P+Tpi/EjEdQu4hAa24LiKxHolWI7JyX
    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.

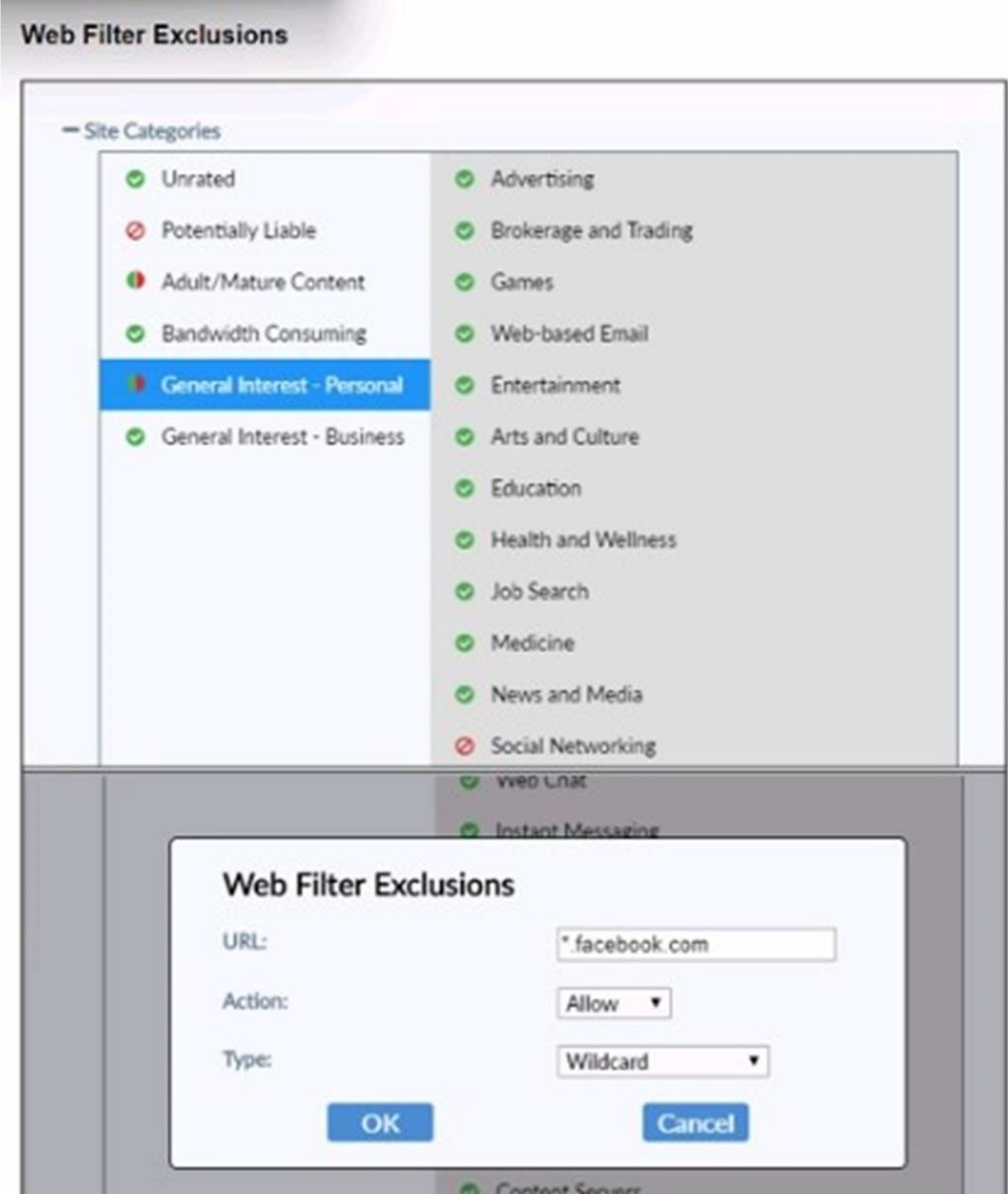
Answer: A

Explanation:

Based on the CLI output from FortiGate:
? The configuration shows the use of "type fortiems," indicating that FortiGate is set up to interact with FortiClient EMS.
? The "server" field points to an IP address (10.0.1.200), which is typically the address of the FortiClient EMS server.
? The configuration includes an SSL-enabled connection, which is a common setup for secure communication between FortiGate and FortiClient EMS.
Thus, the configuration indicates that FortiGate is set up to pull user groups from FortiClient EMS.
References
? FortiGate Security 7.2 Study Guide, FSSO Configuration Section
? Fortinet Documentation on FortiGate and FortiClient EMS Integration

NEW QUESTION 17

Refer to the exhibit.



Based on the settings shown in the exhibit, which action will FortiClient take when users try to access www.facebook.com?

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

Answer: B

Explanation:

? Observation of Web Filter Exclusions:

? Evaluating Actions:

? Conclusion:

References:

? FortiClient web filter configuration and exclusion documentation from the study guides.

NEW QUESTION 20

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCP_FCT_AD-7.2 Practice Exam Features:

- * FCP_FCT_AD-7.2 Questions and Answers Updated Frequently
- * FCP_FCT_AD-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FCT_AD-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FCT_AD-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FCT_AD-7.2 Practice Test Here](#)