

Fortinet

Exam Questions FCP_FCT_AD-7.2

FCP-FortiClient EMS 7.2 Administrator



NEW QUESTION 1

What is the function of the quick scan option on FortiClient?

- A. It scans programs and drivers that are currently running, for threats
- B. It performs a full system scan including all files, executable file
- C. DLLs, and drivers for threats.
- D. It allows users to select a specific file folder on their local hard disk drive (HDD), to scan for threats.
- E. It scans executable file
- F. DLLs, and drivers that are currently running, for threats.

Answer: B

Explanation:

? Understanding Quick Scan Function:

? Evaluating Scan Scope:

? Conclusion:

References:

? FortiClient scanning options documentation from the study guides.

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.

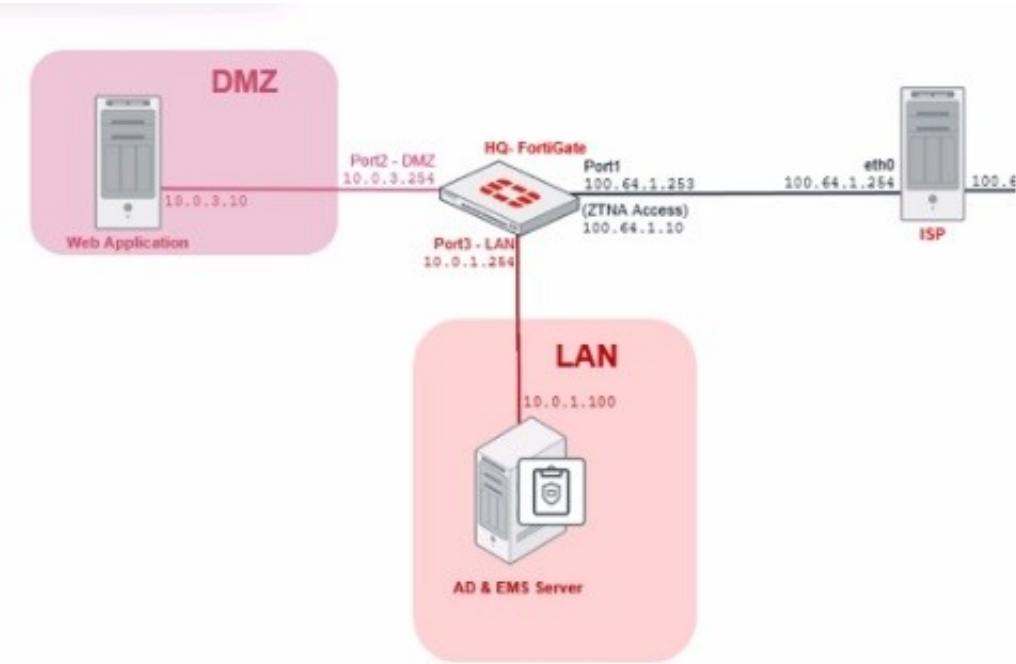
References

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

? Fortinet Documentation on FortiGate Explicit Proxy and ZTNA Integration

NEW QUESTION 3

ZTNA Network Topology



ZTNA Rule Configuration

Name: ZTNA-Allow

Source: all

Negate Source: ☐

ZTNA Tag: Remote-Users

ZTNA Server: ZTNA-webserver

Negate Destination: ☐

Action: ☒ ACCEPT ☐ DENY

Security Profiles

Antivirus: ☐

Web Filter: ☐

Video Filter: ☐

Application Control: ☐

IPS: ☐

File Filter: ☐

SSL Inspection: ssl no-inspection

Logging Options

Log Allowed Traffic: ☒ Security Events ☒ All Sessions

Comments: Write a comment... 0/1023

Enable this policy: ☒

Refer to the exhibits, which show a network topology diagram of ZTNA proxy access and the ZTNA rule configuration. An administrator runs the diagnose endpoint record list CLI command on FortiGate to check Remote-Client endpoint information, however Remote-Client is not showing up in the endpoint record list. What is the cause of this issue?

- A. Remote-Client has not initiated a connection to the ZTNA access proxy.
- B. Remote-Client provided an empty client certificate to connect to the ZTNA access proxy.
- C. Remote-Client provided an invalid certificate to connect to the ZTNA access proxy.
- D. Remote-Client failed the client certificate authentication.

Answer: D

NEW QUESTION 4
Refer to the exhibit.

```
xx/xx/20xx 9:05:05 AM Notice Firewall date=20xx-xx-xx time=09:05:04 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62401 direction=outbound destinationip=199.59.148.82 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Twitter vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy="default" service=http

xx/xx/20xx 9:05:54 AM Notice Firewall date=20xx-xx-xx time=09:05:53 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62425 direction=outbound destinationip=104.25.62.28 remotename=N/A
destinationport=443 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked
utmevent=appfirewall threat=Proxy.Websites vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit
(build 9600)" usingpolicy="default" service=https

xx/xx/20xx 9:28:23 AM Notice Firewall date=20xx-xx-xx time=09:28:22 logver=2 type=traffic level=notice sessionid=26453064
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62759 direction=outbound destinationip=208.71.44.31 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Yahoo.Games vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy="default" service=http
```

Based on the FortiClient logs shown in the exhibit which application is blocked by the application firewall?

- A. Twitter
- B. Facebook
- C. Internet Explorer
- D. Firefox

Answer: D

Explanation:

Based on the FortiClient logs shown in the exhibit:

? The first log entry shows the application "firefox.exe" trying to access a destination IP, with the threat identified as "Twitter."

? The action taken by the application firewall is "blocked" with the event type "appfirewall."

This indicates that the application firewall has blocked access to Twitter.

References

? FortiClient EMS 7.2 Study Guide, Application Firewall Logs Section

? Fortinet Documentation on Interpreting FortiClient Logs

NEW QUESTION 5

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

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

Answer: BDE

Explanation:

? Understanding FortiClient Features:

? Evaluating Feature Set:

? Eliminating Incorrect Options:

References:

? FortiClient endpoint security features documentation from the study guides.

NEW QUESTION 6

Refer to the exhibit, which shows the output of the ZTNA traffic log on FortiGate.

```
eventtime=1633084101662546935 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=100.64.2.253 srcport=58664 srcintf="port1"
srcintfrole="wan" dstip=100.64.1.10 dstport=9443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=5215 proto=6 action="deny" policyid=0
policytype="proxy-policy" service="tcp/9443"trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
rcvdpkt=0 appcat="unscanned" utmaction="block" countstna=1 msg="Denied: failed to match a proxy-policy"
utmref=65462-14
```

What can you conclude from the log message?

- A. The remote user connection does not match the local-in policy.
- B. The remote user connection does not match the ZTNA rule configuration.
- C. The remote user connection does not match the ZTNA server configuration.
- D. The remote user connection does not match the ZTNA firewall policy.

Answer: B

Explanation:

? Observation of ZTNA Traffic Log:

? Evaluating Log Message:
? Conclusion:
References:
? ZTNA traffic log analysis and configuration documentation from the study guides.

NEW QUESTION 7

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-EHVK8EA3S71 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. 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 8


Refer to the exhibits.

Security Fabric Settings

☒ FortiGate Telemetry


Security Fabric role Serve as Fabric Root Join Existing Fabric


Fabric name

Topology  FGVM010000052731 (Fabric Root)

Allow other FortiGates to join ☒ port3 + ×

Pre-authorized FortiGates None Edit

SAML Single Sign-On  ☐

Management IP/FQDN  Use WAN IP Specify

Management Port Use Admin Port Specify

☒ FortiAnalyzer Logging

IP address


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  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 ×

IP/Domain Name

Serial Number

Admin User

Password •••••••• Change

+

The screenshot shows the FortiGate Security Fabric settings for EMS integration. The fields are as follows:

- Hostname:** EMSServer
- Listen on IP:** 10.0.1.100 (with a refresh icon)
- Use FQDN:** ☒ (checked)
- FQDN:** myemsserver
- Remote HTTPS access:** ☐ (unchecked)
- SSL certificate:** No certificate imported (with an upload icon)

Below the Listen on IP field, there is a note: "FQDN is required when listening to all IPs." Below the Remote HTTPS access field, there is a note: "Only enforced when Windows Firewall is running."

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 (IoC)?

- 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.

Answer: A

Explanation:

Based on the FortiGate Security Fabric settings shown in the exhibits, to successfully quarantine an endpoint when it is detected as a compromised host (IOC), the following step is required:

? Enable Remote HTTPS Access to EMS: This setting allows FortiGate to communicate securely with FortiClient EMS over HTTPS. Remote HTTPS access is essential for the quarantine functionality to operate correctly, enabling the EMS server to receive and act upon the quarantine commands from FortiGate. Therefore, the administrator must enable remote HTTPS access to EMS to allow the quarantine process to function properly.

References

- ? FortiGate Infrastructure 7.2 Study Guide, Security Fabric and Integration with EMS Sections
- ? Fortinet Documentation on Enabling Remote HTTPS Access to FortiClient EMS

NEW QUESTION 9

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 10

Refer to the exhibit.

Edit Automation Stitch

Name
Stitch


Status

Enabled
Disabled

FortiGate

All FortiGates

Trigger



Compromised Host

Threat level threshold

Medium
High

Action

CLI Script

Email

FortiExplorer Notification

Access Layer Quarantine

Quarantine FortiClient via EMS

Assign VMware NSX Security Tag

IP Ban

AWS Lambda

Azure Function

Google Cloud Function

AliCloud Function

Webhook

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

Answer: A

Explanation:

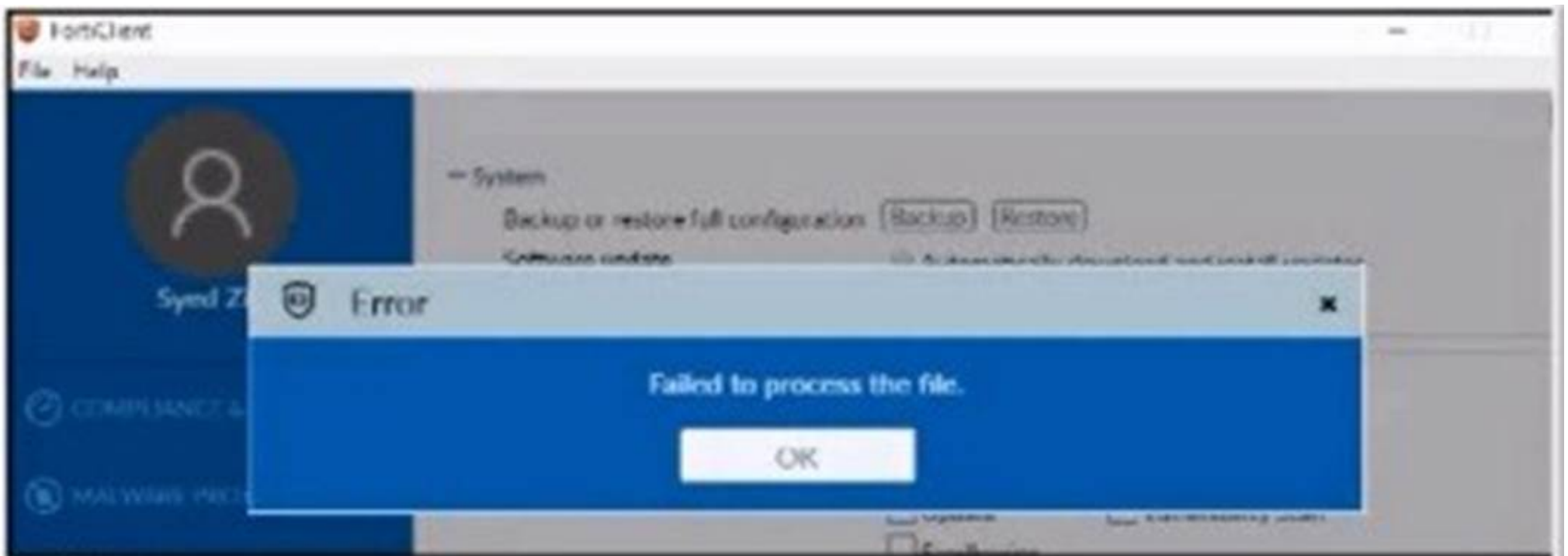
Based on the Security Fabric automation settings shown in the exhibit:
 ? The automation stitch is configured with a trigger for a "Compromised Host."
 ? The action specified for this trigger is "Quarantine FortiClient via EMS."
 ? This indicates that when an endpoint is detected as compromised, FortiClient EMS will quarantine the endpoint as part of the automation process.
 Therefore, the action taken on compromised endpoints will be to quarantine them through EMS.

References

- ? FortiGate Security 7.2 Study Guide, Automation Stitches and Actions Section
- ? Fortinet Documentation on Configuring Automation Stitches and Quarantine Actions

NEW QUESTION 10

Refer to the exhibit.



```
<sslvpn>
  <options>
    <enabled>1</enabled>
    <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
    <dnscache_service_control>0</dnscache_service_control>
    <use_legacy_ssl_adapter>0</use_legacy_ssl_adapter>
    <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
    <no_dhcp_server_route>0</no_dhcp_server_route>
    <no_dns_registration>0</no_dns_registration>
    <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
  </options>
  <connections>
    <connection>
      <name>Student-SSLVPN</name>
      <description>SSL VPN to Fortigate</description>
      <server>10.0.0.254:10443</server>
      <username />
      <single_user_mode>0</single_user_mode>
      <ui>
        <show_remember_password>0</show_remember_password>
      </ui>
      <password />
      <prompt_username>1</prompt_username>
      <on_connect>
        <script>
          <os>windows</os>
          <script>
            <![CDATA[]]>
          </script>
        </script>
      </on_connect>
      <on_disconnect>
        <script>
          <os>windows</os>
          <script>
            <![CDATA[]]>
          </script>
        </script>
      </on_disconnect>
    </connection>
  </connections>
</sslvpn>
```

An administrator has restored the modified XML configuration file to FortiClient and sees the error shown in the exhibit. Based on the XML settings shown in the exhibit, what must the administrator do to resolve the issue with the XML configuration file?

- A. The administrator must resolve the XML syntax error.
- B. The administrator must use a password to decrypt the file
- C. The administrator must change the file size
- D. The administrator must save the file as FortiClient-config conf.

Answer: A

Explanation:

Based on the error message and the XML configuration file shown in the exhibit:

? The error "Failed to process the file" typically indicates an issue with the XML syntax.

? Upon reviewing the XML content, it is crucial to ensure that all tags are correctly formatted, properly opened and closed, and that there are no syntax errors.

? Resolving any XML syntax errors will allow FortiClient to successfully process and restore the configuration file.

Therefore, the administrator must resolve the XML syntax error to fix the issue.

References

? FortiClient EMS 7.2 Study Guide, Configuration File Management Section

? General XML Syntax Guidelines and Best Practices

NEW QUESTION 13

.....

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](#)