



Fortinet

Exam Questions FCP_FCT_AD-7.2

FCP-FortiClient EMS 7.2 Administrator

NEW QUESTION 1

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

Answer: BC

Explanation:

Administrators can use several third-party tools to deploy FortiClient:

? Microsoft SCCM (System Center Configuration Manager): SCCM is a robust tool used for deploying software across large numbers of Windows-based systems. It supports deployment of FortiClient through its software distribution capabilities.

? Microsoft Active Directory GPO (Group Policy Object): GPOs are used to manage user and computer settings in an Active Directory environment. Administrators can deploy FortiClient to multiple machines using GPO software installation settings.

These tools provide centralized and scalable methods for deploying FortiClient across numerous endpoints in an enterprise environment.

References

? FortiClient EMS 7.2 Study Guide, FortiClient Deployment Section

? Fortinet Documentation on FortiClient Deployment using SCCM and GPO

NEW QUESTION 2

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

- A. It applies security profiles to protect traffic
- B. It applies SNAT to protect traffic.
- C. It defines the access proxy.
- D. It enforces access control.

Answer: AD

Explanation:

? Understanding ZTNA Rule Configuration:

? Evaluating Rule Components:

? Eliminating Incorrect Options:

? Conclusion:

References:

? ZTNA rule configuration documentation from the study guides.

NEW QUESTION 3

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

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

Answer: A

Explanation:

? Understanding the Need for Root CA Certificate:

? Evaluating Use Cases:

? Conclusion:

References:

? FortiClient EMS and FortiGate certificate management documentation from the study guides.

NEW QUESTION 4

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.

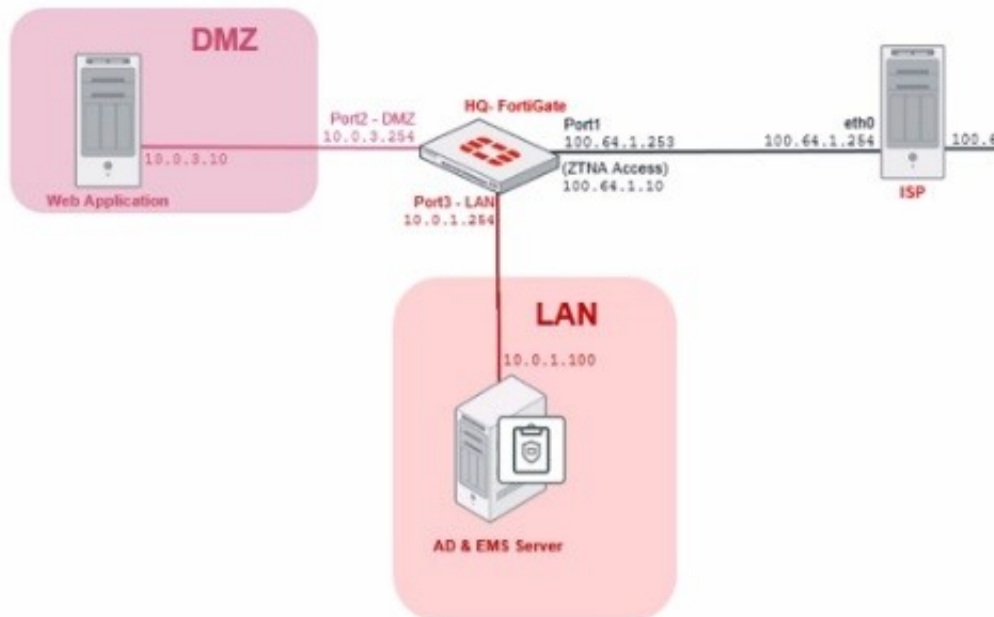
References

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

? Fortinet Documentation on FortiGate Explicit Proxy and ZTNA Integration

NEW QUESTION 5

ZTNA Network Topology



ZTNA Rule Configuration

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: 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 6

An administrator configures ZTNA configuration on the FortiGate. Which statement is true about the firewall policy?

- A. It redirects the client request to the access proxy.
- B. It uses the access proxy.
- C. It defines ZTNA server.
- D. It only uses ZTNA tags to control access for endpoints.

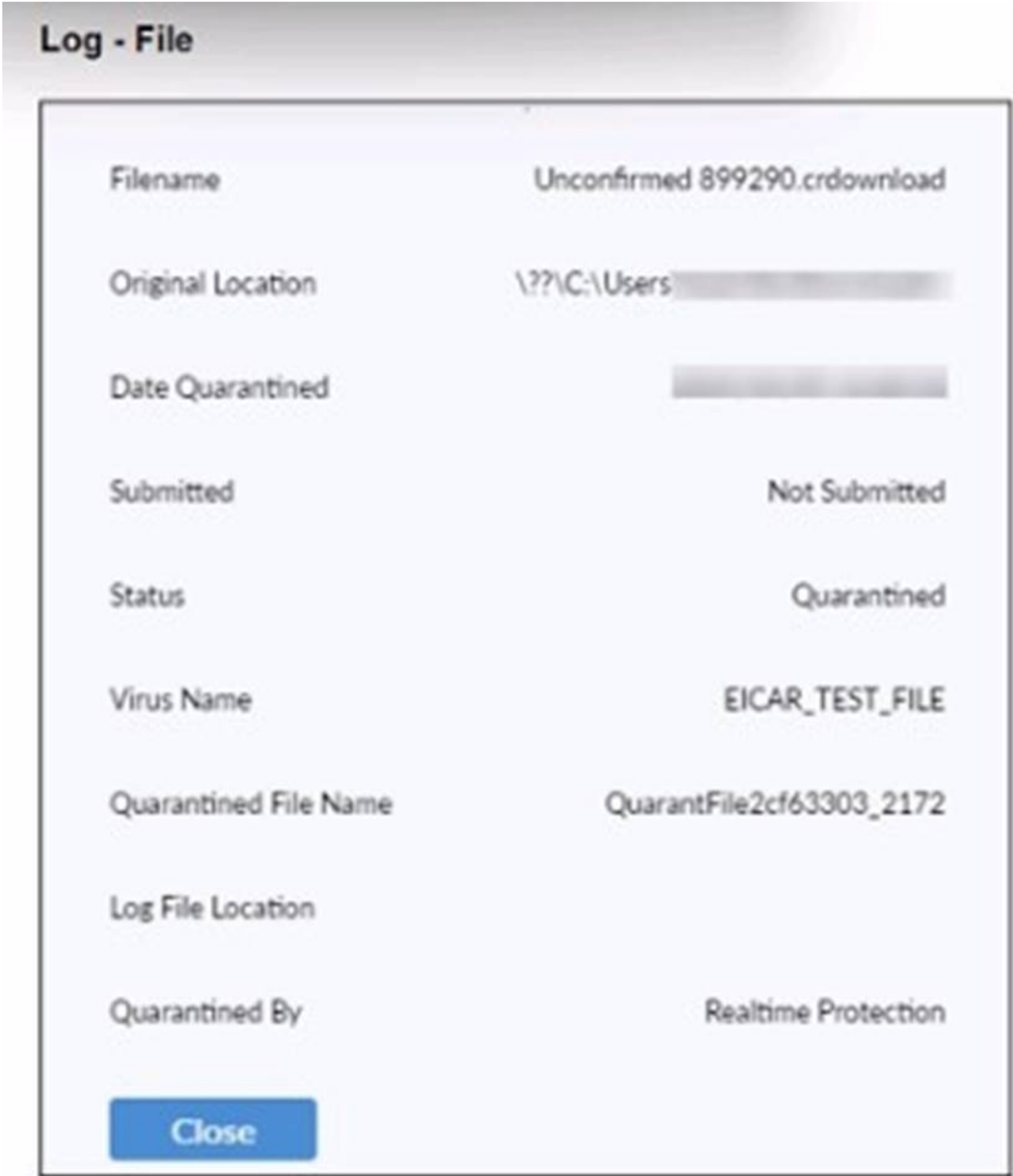
Answer: A

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>

NEW QUESTION 7

Refer to the exhibit.



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 8

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 9

Which component or device defines ZTNA lag information in the Security Fabric integration?

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

Answer: C

Explanation:

? Understanding ZTNA:
? Evaluating Components:
? Conclusion:
References:
? ZTNA and FortiClient EMS configuration documentation from the study guides.

NEW QUESTION 10

Refer to the exhibit, which shows FortiClient EMS deployment, profiles.

Deployments						+ Add	Change Priority
Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled		
Deployment-1	All Groups	First-Time-Installation		1	<input type="checkbox"/>		
Deployment-2	All Groups trainingAD.training.lab	To-Upgrade		2	<input checked="" type="checkbox"/>		

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

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

Answer: A

Explanation:

? Deployment Profiles Analysis:
? Evaluating Deployment-2:
? Conclusion:
References:
? FortiClient EMS deployment and profile documentation from the study guides.

NEW QUESTION 10

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 15

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 >

Zero Trust Tags 2 **Outbreak Tags** 0 **Classification** 1

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 TELEMETRY

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 18

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 23

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 24

An administrator must add an authentication server on FortiClient EMS in a different security zone that cannot allow a direct connection. Which solution can provide secure access between FortiClient EMS and the Active Directory server?

- A. Configure and deploy a FortiGate device between FortiClient EMS and the Active Directory server.
- B. Configure Active Directory and install FortiClient EMS on the same VM.
- C. Configure a slave FortiClient EMS on a virtual machine.
- D. Configure an Active Directory connector between FortiClient EMS and the Active Directory server.

Answer: A

Explanation:

? Requirement:

? Solution Analysis:

? Evaluating Options:

? Conclusion:

References:

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

NEW QUESTION 29

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

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

Answer: A

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.

References :=

? 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

NEW QUESTION 34


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

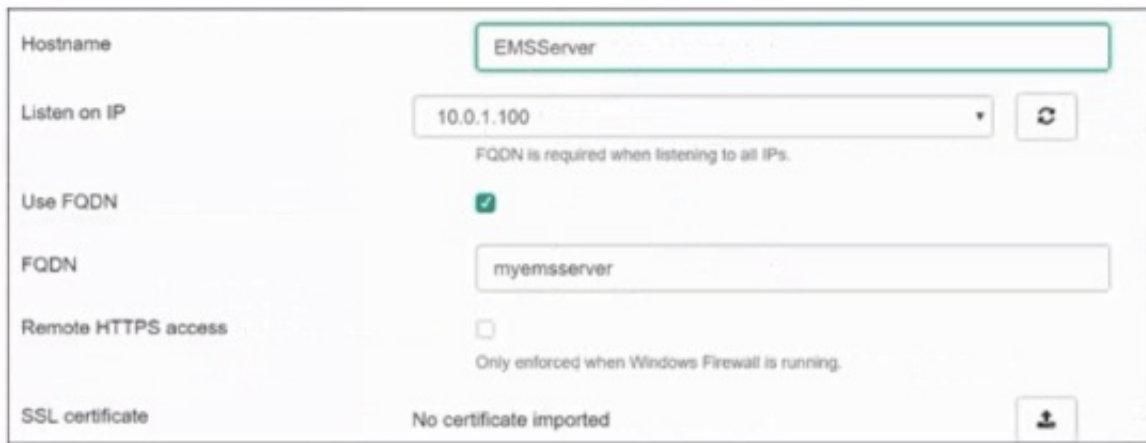
Admin User

Password

••••••••

Change

+



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 35

Which two VPN types can a FortiClient endpoint user initiate from the Windows command prompt? (Choose two)

- A. L2TP
- B. PPTP
- C. IPsec
- D. SSL VPN

Answer: CD

Explanation:

FortiClient supports initiating the following VPN types from the Windows command prompt:

? IPsec VPN: FortiClient can establish IPsec VPN connections using command line instructions.

? SSL VPN: FortiClient also supports initiating SSL VPN connections from the Windows command prompt.

These two VPN types can be configured and initiated using specific command line parameters provided by FortiClient.

References

? FortiClient EMS 7.2 Study Guide, VPN Configuration Section

? Fortinet Documentation on Command Line Options for FortiClient VPN

NEW QUESTION 37

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 42

Which three types of antivirus scans are available on FortiClient? (Choose three)

- A. Proxy scan
- B. Full scan
- C. Custom scan
- D. Flow scan
- E. Quick scan

Answer: BCE

Explanation:

FortiClient offers several types of antivirus scans to ensure comprehensive protection:

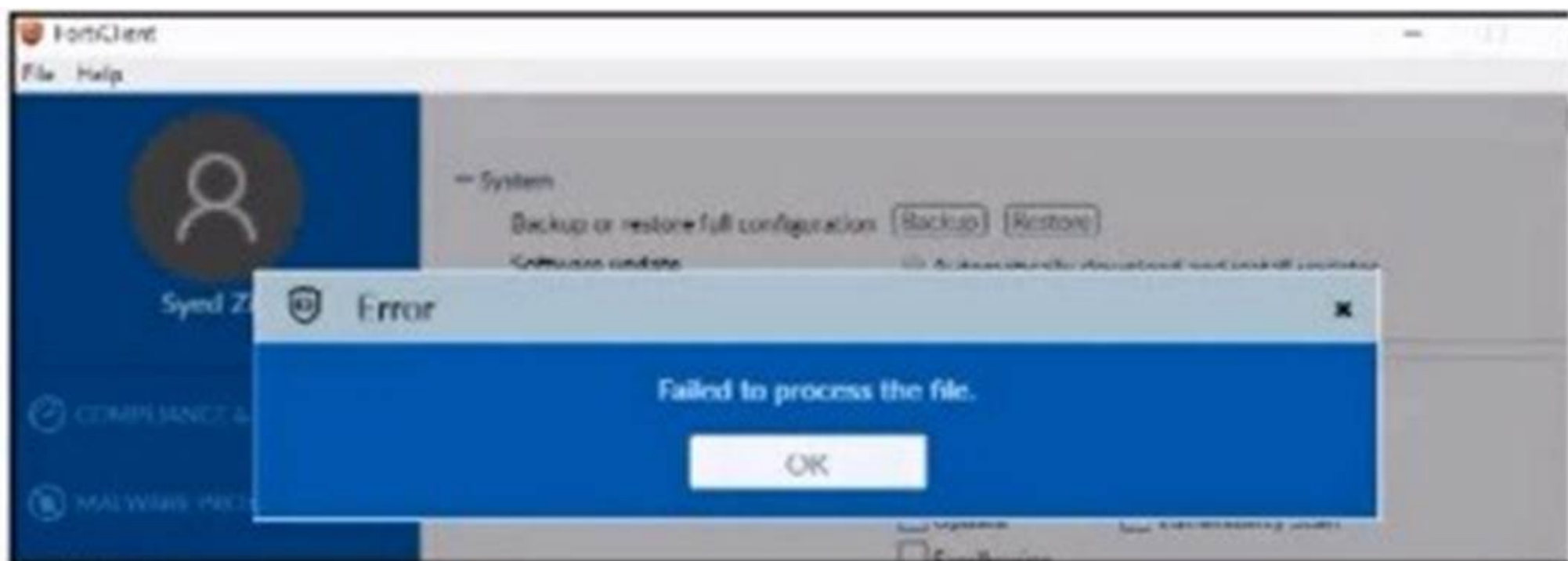
- ? Full scan: Scans the entire system for malware, including all files and directories.
 - ? Custom scan: Allows the user to specify particular files, directories, or drives to be scanned.
 - ? Quick scan: Scans the most commonly infected areas of the system, providing a faster scanning option.
- These three types of scans provide flexibility and thoroughness in detecting and managing malware threats.

References

? FortiClient EMS 7.2 Study Guide, Antivirus Scanning Options Section
? Fortinet Documentation on Types of Antivirus Scans in FortiClient

NEW QUESTION 45

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 50

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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](#)