



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

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 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.

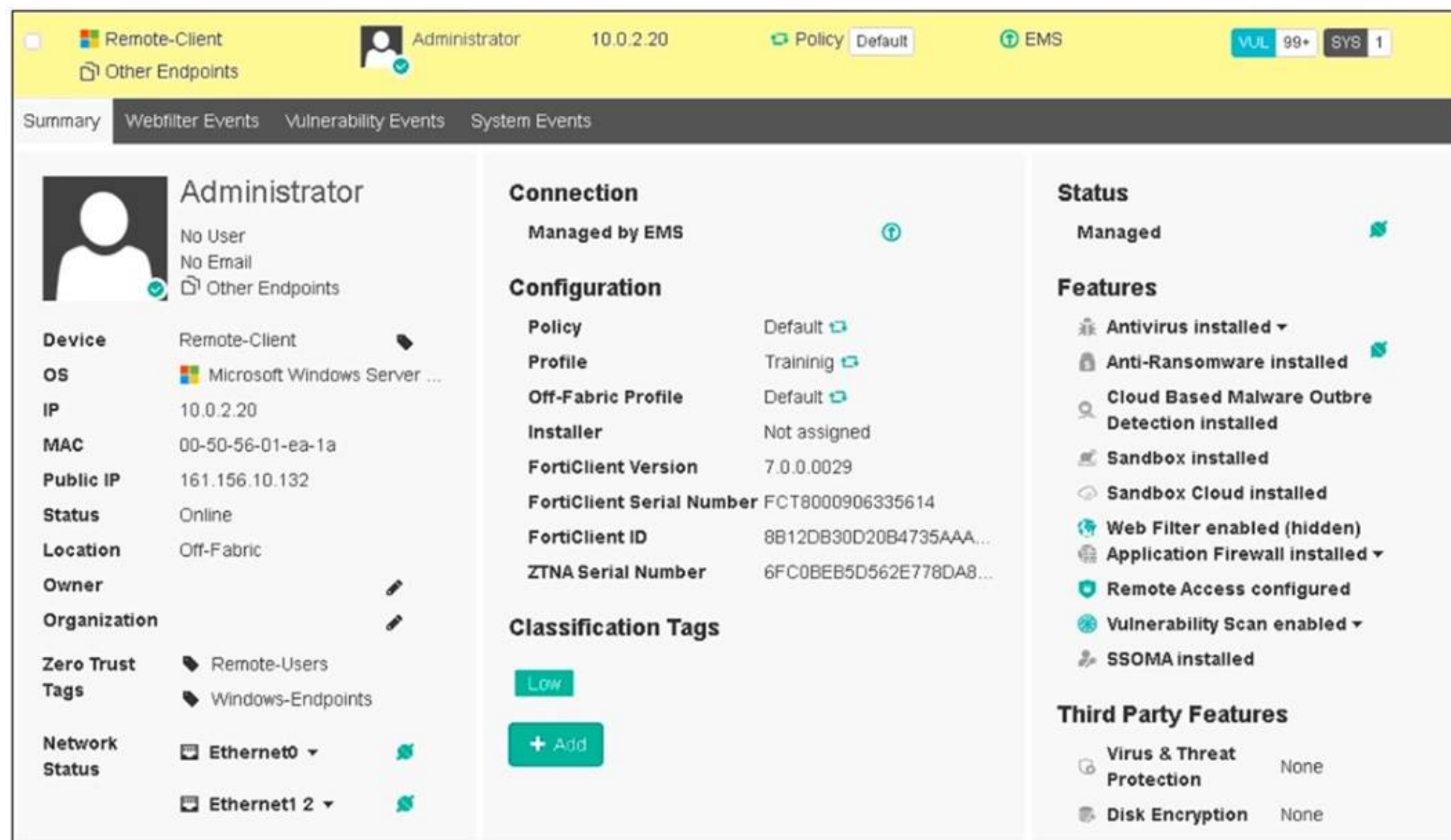
Answer: A

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 5

Refer to the exhibit, which shows the endpoint summary information on FortiClient EMS.



The screenshot displays the FortiClient EMS 7.2 interface. At the top, a yellow header bar shows the user 'Administrator' with a profile icon, the version '10.0.2.20', and tabs for 'Policy' (Default) and 'EMS'. On the right, there are status indicators for 'VUL' (99+) and 'SYS' (1). Below the header, a navigation bar includes 'Summary', 'Webfilter Events', 'Vulnerability Events', and 'System Events'. The main content area is divided into three columns:

- Left Column (Endpoint Details):** Shows a profile icon for 'Administrator' with 'No User' and 'No Email' status. Below this, a table lists device information: Device (Remote-Client), OS (Microsoft Windows Server ...), IP (10.0.2.20), MAC (00-50-56-01-ea-1a), Public IP (161.156.10.132), Status (Online), Location (Off-Fabric), Owner (blank), Organization (blank), Zero Trust Tags (Remote-Users, Windows-Endpoints), and Network Status (Ethernet0, Ethernet1 2).
- Middle Column (Configuration & Classification):** Includes a 'Connection' section stating 'Managed by EMS'. The 'Configuration' section lists: Policy (Default), Profile (Training), Off-Fabric Profile (Default), Installer (Not assigned), FortiClient Version (7.0.0.0029), FortiClient Serial Number (FCT8000906335614), FortiClient ID (8B12DB30D20B4735AAA...), and ZTNA Serial Number (6FC0BEB5D562E778DA8...). The 'Classification Tags' section shows a 'Low' tag and an '+ Add' button.
- Right Column (Status & Features):** Shows 'Status' as 'Managed'. The 'Features' section lists: Antivirus installed, Anti-Ransomware installed, Cloud Based Malware Outbreak Detection installed, Sandbox installed, Sandbox Cloud installed, Web Filter enabled (hidden), Application Firewall installed, Remote Access configured, Vulnerability Scan enabled, and SSOMA installed. The 'Third Party Features' section shows 'Virus & Threat Protection' and 'Disk Encryption' both set to 'None'.

What two conclusions can you make based on the Remote-Client status shown above? (Choose two.)

- A. The endpoint is classified as at risk.
- B. The endpoint has been assigned the Default endpoint policy.
- C. The endpoint is configured to support FortiSandbox.
- D. The endpoint is currently off-net.

Answer: BD

Explanation:

Based on the Remote-Client status shown in the exhibit:

? Endpoint Policy: The "Policy" field shows "Default," indicating that the endpoint has been assigned the Default endpoint policy.

? Connection Status: The "Location" field shows "Off-Fabric," meaning that the endpoint is currently off the corporate network (off-net).

Therefore, the two conclusions that can be made are:

? The endpoint has been assigned the Default endpoint policy.

? The endpoint is currently off-net.

References

? FortiClient EMS 7.2 Study Guide, Endpoint Summary Information Section

? Fortinet Documentation on Endpoint Policies and Status Indicators

NEW QUESTION 6

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 7

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 8

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 9

Which two statements are true about ZTNA? {Choose two.}

A. ZTNA manages access for remote users only.

B. ZTNA provides role-based access.

C. ZTNA provides a security posture check.

D. ZTNA manages access through the client only.

Answer: BC

Explanation:

ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of "never trust, always verify," which means that all access to network resources is subject to strict verification and authentication.

Two functions of ZTNA are:

ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the

device's software and hardware configurations, security settings, and the presence of malware.

ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data breaches.

NEW QUESTION 10

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

A. Deny access to a file when it sees no results

B. Alert and notify only

C. Exclude specified files

D. Wait for FortiSandbox results before allowing files

Answer: B

Explanation:

? Understanding FortiSandbox Integration:

? Evaluating Remediation Options:

? Conclusion:

References:

? FortiSandbox integration documentation from the study guides.

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 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 15

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

Answer: C

Explanation:

? Understanding Compliance Rules:

? Enforcing Compliance:

? Conclusion:

References:

? Compliance and enforcement documentation from FortiGate and FortiClient EMS study guides.

NEW QUESTION 20

Which security fabric component sends a notification to quarantine an endpoint after IOC detection in the automation process?

- A. FortiAnalyzer
- B. FortiClient
- C. FortiClient EMS
- D. Forti Gate

Answer: D

NEW QUESTION 24

FortiClient EMS endpoint policies

Endpoint Policies									
+ Add Change Priority Refresh Clear Filters Edit									
Name	Assigned Groups	Profile Components	Policy Components	Endpoint Count	Priority	Enabled			
Sales	All Groups trainingAD.training.lab	VPN Training WEB Training MW Training FW Training	ZTNA Training VULN Training SB Training SYS Training	ON-FABRIC On-Fabric	1				
Training	trainingAD.training.lab	VPN Training WEB Training MW Training FW Training	ZTNA Training VULN Training SB Training SYS Training	ON-FABRIC On-Fabric	1	2			
Default		VPN Default WEB Default MW Default FW Default	ZTNA Default VULN Default SB Default SYS Default	ON-FABRIC On-Fabric	1	3			

Refer to the exhibit, which shows multiple endpoint policies on FortiClient EMS. Which policy is applied to the endpoint in the AD group trainingAD

- A. The Training policy
- B. Both the Sales and Training policies because their priority is higher than the Default policy
- C. The Default policy because it has the highest priority
- D. The sales policy

Answer: A

Explanation:

- ? Observation of Endpoint Policies:
- ? Evaluating Policy Assignment:
- ? Conclusion:
- References:
- ? FortiClient EMS policy configuration and priority management documentation from the study guides.

NEW QUESTION 26

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

Scan Now

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

Answer: D

Explanation:

- Block Malicious Website has nothing to do with infected files. Since Realtime Protection is OFF, it will be allowed without being scanned.
- Based on the settings shown in the exhibit:
- ? Realtime Protection:OFF
 - ? Dynamic Threat Detection:OFF
 - ? Block malicious websites:ON
 - ? Threats Detected:75
- The "Realtime Protection" setting is crucial for preventing infected files from being downloaded and executed. Since "Realtime Protection" is OFF, FortiClient will not actively scan files being downloaded. The setting "Block malicious websites" is intended to prevent access to known malicious websites but does not scan files for infections.
- Therefore, when a user tries to download an infected file, FortiClient will allow the file to download without scanning it due to the Realtime Protection being OFF.
- References
- ? FortiClient EMS 7.2 Study Guide, Antivirus Protection Section
 - ? Fortinet Documentation on FortiClient Real-time Protection Settings

NEW QUESTION 27

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. It helps to safeguard systems from advanced security threats, such as malware.

Answer: D

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.

NEW QUESTION 32

.....

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](#)