# Free Questions for NSE7_ZTA-7.2 by certsdeals

## Shared by Brennan on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

**Question Type: MultipleChoice**

Which configuration is required for FortiNAC to perform an automated incident response based on the FortiGate traffic?

## Options:

**A-** FortiNAC should be added as a participant in the Security Fabric

**B-** FortiNAC requires read-write SNMP access to FortiGate.

**C-** FortiNAC should be configured as a syslog server on FortiGate

**D-** FortiNAC requires HTTPS access to FortiGate for API calls

## Answer:

A

## Explanation:

For FortiNAC to perform automated incident response based on FortiGate traffic, the required configuration is:

A) FortiNAC should be added as a participant in the Security Fabric: By integrating FortiNAC into the Fortinet Security Fabric, it can respond to incidents based on traffic analysis performed by FortiGate. This allows for coordinated and automated responses to security events.

The other options are not specifically required for automated incident response in this context:

B) FortiNAC requires read-write SNMP access to FortiGate: While SNMP access is important for certain functions, it is not the key requirement for this

specific use case.

C) FortiNAC should be configured as a syslog server on FortiGate: Configuring FortiNAC as a syslog server is useful for log collection but not specifically for automated incident response based on traffic.

D) FortiNAC requires HTTPS access to FortiGate for API calls: HTTPS access for API calls is important for integration, but it is not the primary requirement for automated incident response based on FortiGate traffic analysis.

FortiNAC Integration with FortiGate for Incident Response.

Fortinet Security Fabric Documentation.

## Question 2

**Question Type:** **MultipleChoice**

Which factor is a prerequisite on FortiNAC to add a Layer 3 router to its inventory?

## Options:

**A-** Allow HTTPS access from the router to the FortiNAC ethO IP address

**B-** Allow FTP access to the FortiNAC database from the router

**C-** The router responding to ping requests from the FortiNAC eth1 IP address

**D-** SNMP or CLI access to the router to carry out remote tasks

## Answer:

D

## Explanation:

FortiNAC uses SNMP or CLI to communicate with network devices such as routers and switches. To add a Layer 3 router to its inventory, FortiNAC needs to have SNMP or CLI access to the router to perform remote tasks such as polling, VLAN assignment, and port shutdown. Without SNMP or CLI access, FortiNAC cannot manage the router or its ports.Therefore, SNMP or CLI access is a prerequisite for adding a Layer 3 router to FortiNAC's inventory.Reference:= https://docs.fortinet.com/document/fortinac/9.4.0/administration-guide/105927/inventory

https://docs.fortinet.com/document/fortinac/9.4.0/administration-guide/344098/l3-polling

# Question 3

**Question Type: MultipleChoice**

An administrator is trying to create a separate web tittering profile for off-fabric and on-fabric clients and push it to managed FortiClient devices

Where can you enable this feature on FortiClient EMS?

## Options:

**A-** Endpoint policy

**B-** ZTNA connection rules

**C-** System settings

**D-** On-fabric rule sets

## Answer:

A

### Explanation:

To create a separate web filtering profile for off-fabric and on-fabric clients and push it to managed FortiClient devices in FortiClient EMS, the feature can be enabled in:

A) Endpoint Policy: This is where administrators can define and manage different policies for FortiClient endpoints. These policies can include settings for web filtering, which can be customized for on-fabric and off-fabric scenarios.

The other options do not directly relate to the creation and management of web filtering profiles:

B) ZTNA Connection Rules: These rules are more focused on access control and do not deal directly with web filtering profiles.

C) System Settings: This section typically includes overall system configurations rather than specific policy definitions.

D) On-fabric Rule Sets: While important for on-fabric configurations, they don't directly deal with web filtering profiles.

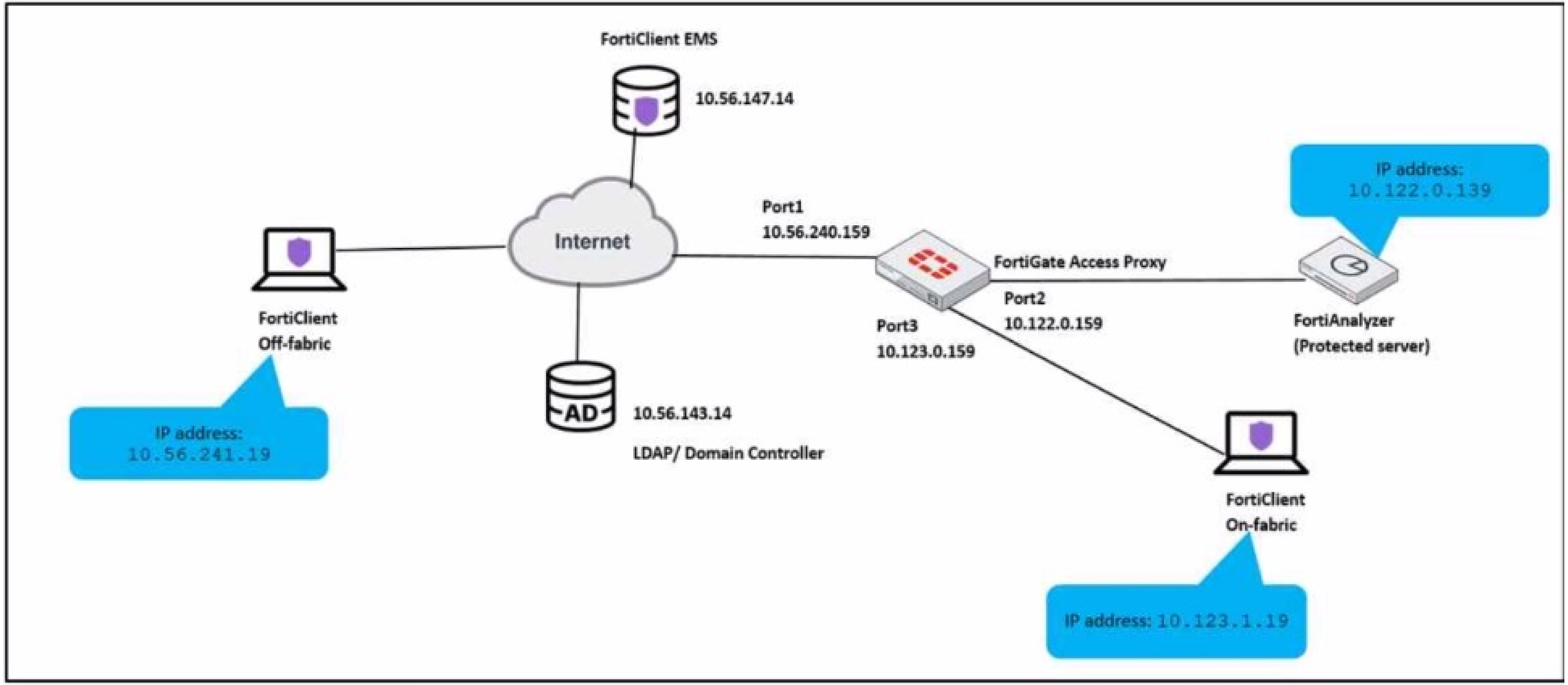
FortiClient EMS Administration Guide.

Managing Endpoint Policies in FortiClient EMS.

## Question 4

**Question Type:** MultipleChoice

Exhibit.



An administrator has to provide on-fabric clients with access to FortiAnalyzer using ZTNA tags

Which two conditions must be met to achieve this task? (Choose two.)

## Options:

**A-** The on-fabric client should have FortiGate as its default gateway

**B-** The ZTNA server must be configured on FortiGate

**C-** The ZTNA rule must be configured on FortiClient

**D-** The IP/MAC based firewall policy must be configured on FortiGate

## Answer:

A, B

## Explanation:

For on-fabric clients to access FortiAnalyzer using ZTNA tags, the following conditions must be met:

A) The on-fabric client should have FortiGate as its default gateway: This is essential to ensure that all client traffic is routed through FortiGate, where ZTNA policies can be enforced.

B) The ZTNA server must be configured on FortiGate: For ZTNA tags to be effectively used, the ZTNA server, which processes and enforces these tags, must be configured on the FortiGate appliance.

Configuring ZTNA tags and tagging rules

Synchronizing FortiClient ZTNA tags

FortiAnalyzer

Technical Tip: ZTNA Tags fail to synchronize between FortiClient and FortiGate

# Question 5

**Question Type: MultipleChoice**

Which three core products are mandatory in the Fortinet ZTNA solution" {Choose three.)

## Options:

**A-** FortiClient EMS

**B-** FortiClient

**C-** FortiToken

**D-** FortiGate

**E-** FortiAuthenticator

## Answer:

A, B, D

### Explanation:

Fortinet ZTNA solution is a zero-trust network access approach that provides secure and granular access to applications hosted anywhere, for users working from anywhere. The three core products that are mandatory in the Fortinet ZTNA solution are:

FortiClient EMS: This is the central management console that orchestrates the ZTNA policies and provides visibility and control over the endpoints and devices. It also integrates with FortiAuthenticator for identity verification and FortiAnalyzer for reporting and analytics.

FortiClient: This is the endpoint agent that supports ZTNA, VPN, endpoint protection, and vulnerability scanning. It establishes encrypted tunnels with the ZTNA proxy on the FortiGate and provides device posture and single sign-on (SSO) capabilities.

FortiGate: This is the next-generation firewall that acts as the ZTNA proxy and enforces the ZTNA policies based on user identity, device posture, and application context. It also provides security inspection and threat prevention for the ZTNA traffic.

# Question 6

**Question Type: MultipleChoice**

Which method is used to install passive agent on an endpoint?

## Options:

**A-** Deployed by using a login/logout script

**B-** Agent is downloaded from Playstore

**C-** Agent is downloaded and run from captive portal

**D-** Installed by user or deployment tools

## Answer:

D

## Explanation:

The method used to install a passive agent on an endpoint is:

D) Installed by user or deployment tools: Passive agents are typically installed on endpoints either manually by users or automatically through deployment tools used by the organization.

The other options do not accurately describe the installation of passive agents:

A) Deployed by using a login/logout script: This is not the standard method for deploying passive agents.

B) Agent is downloaded from Playstore: This is more relevant for mobile devices and does not represent the general method for passive agent installation.

C) Agent is downloaded and run from captive portal: This method is not typically used for installing passive agents.

FortiNAC Agent Deployment Guide.

Installation Methods for Passive Agents in FortiNAC.

## Question 7

**Question Type: MultipleChoice**

Which three methods can you use to trigger layer 2 polling on FortiNAC? (Choose three)

### Options:

**A-** Polling scripts

**B-** Link traps

**C-** Manual polling

**D-** Scheduled tasks

**E-** Polling using API

## Answer:

A, C, D

## Explanation:

To trigger layer 2 polling on FortiNAC, the three methods are:

A) Polling scripts: These are scripts configured within FortiNAC to actively poll the network at layer 2 to gather information about connected devices.

C) Manual polling: This involves manually initiating a polling process from the FortiNAC interface to gather current network information.

D) Scheduled tasks: Polling can be scheduled as regular tasks within FortiNAC, allowing for automated, periodic collection of network data.

The other options are not standard methods for layer 2 polling in FortiNAC:

B) Link traps: These are more related to SNMP trap messages rather than layer 2 polling.

E) Polling using API: While APIs are used for various integrations, they are not typically used for initiating layer 2 polling in FortiNAC.

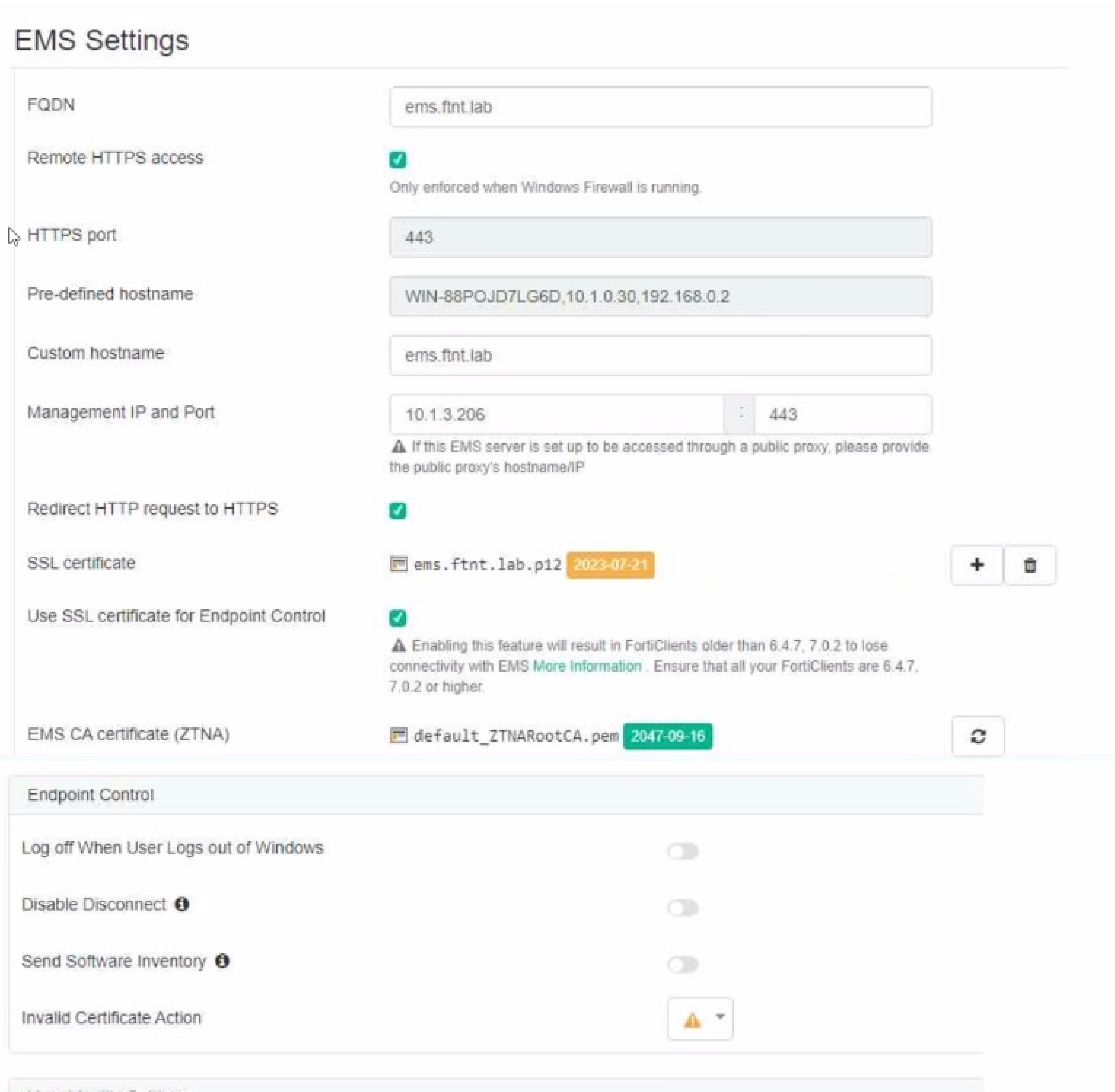
FortiNAC Layer 2 Polling Documentation.

Configuring Polling Methods in FortiNAC.

# Question 8

**Question Type:** **MultipleChoice**

Exhibit.



## EMS Settings

FQDN: ems.ftnt.lab

Remote HTTPS access: ☑

Only enforced when Windows Firewall is running.

HTTPS port: 443

Pre-defined hostname: WIN-88POJD7LG6D,10.1.0.30,192.168.0.2

Custom hostname: ems.ftnt.lab

Management IP and Port: 10.1.3.206 : 443

⚠ If this EMS server is set up to be accessed through a public proxy, please provide the public proxy's hostname/IP

Redirect HTTP request to HTTPS: ☑

SSL certificate: `ems.ftnt.lab.p12` 2023-07-21

Use SSL certificate for Endpoint Control: ☑

⚠ Enabling this feature will result in FortiClients older than 6.4.7, 7.0.2 to lose connectivity with EMS More Information . Ensure that all your FortiClients are 6.4.7, 7.0.2 or higher.

EMS CA certificate (ZTNA): `default_ZTNARootCA.pem` 2047-09-16

### Endpoint Control

Log off When User Logs out of Windows: ○

Disable Disconnect: ○

Send Software Inventory: ○

Invalid Certificate Action: ⚠

Which statement is true about the configuration shown in the exhibit?

## Options:

**A-** The domain that FortiClient is connecting to should match the domain to which the certificate is issued.

**B-** It the FortiClient EMS server certificate is invalid, FortiClient connects silently.

**C-** The connection from FortiClient to FortiClient EMS uses TCP and TLS 1.2.

**D-** default_ZTNARoot CA signs the FortiClient certificate for the SSL connectivity to FortiClient EMS

## Answer:

C

## Explanation:

The exhibit shows the EMS Settings where various configurations related to network security are displayed. Option C is correct because, in the settings, it is indicated that HTTPS port is used (which operates over TCP) and SSL certificates are involved in securing the connection, implying the use of TLS for encryption and secure communication between FortiClient and FortiClient EMS.

Option A is incorrect because the domain that FortiClient is connecting to does not have to match the domain to which the certificate is issued. The certificate is issued by the ZTNA CA, which is a separate entity from the domain. The certificate only contains the device ID, ZTNA tags, and other information that are used to identify and authenticate the device.

Option B is incorrect because if the FortiClient EMS server certificate is invalid, FortiClient does not connect silently. Instead, it performs the Invalid Certificate Action that is configured in the settings. The Invalid Certificate Action can be set to block, warn, or allow the connection.

Option D is incorrect because default_ZTNARoot CA does not sign the FortiClient certificate for the SSL connectivity to FortiClient EMS. The FortiClient certificate is signed by the ZTNA CA, which is a different certificate authority from default_ZTNARoot CA. default_ZTNARoot CA is the EMS CA Certificate that is used to verify the identity of the EMS server.

[1]: Technical Tip: ZTNA for Corporate hosts with SAML authentication and FortiAuthenticator as IDP

[2]: Zero Trust Network Access - Fortinet

# Question 9

**Question Type: MultipleChoice**

Which statement is true regarding a FortiClient quarantine using FortiAnalyzer playbooks?

## Options:

**A-** FortiGate sends a notification to FortiClient EMS to quarantine the endpoint

**B-** FortiAnalyzer discovers malicious activity in the logs and notifies FortiGate

**C-** FortiAnalyzer sends an API to FortiClient EMS to quarantine the endpoint

**D-** FortiClient sends logs to FortiAnalyzer

### Answer:

C

### Explanation:

FortiAnalyzer playbooks are automated workflows that can perform actions based on triggers, conditions, and outputs. One of the actions that a playbook can perform is to quarantine a device by sending an API call to FortiClient EMS, which then instructs the FortiClient agent on the device to disconnect from the network. This can help isolate and contain a compromised or non-compliant device from spreading malware or violating policies.Reference:=

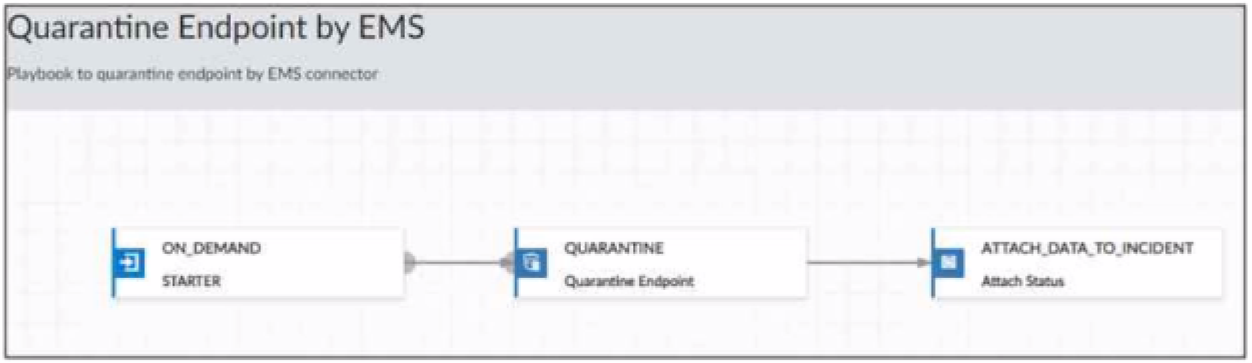
Quarantine a device from FortiAnalyzer playbooks

Playbooks

## Question 10

**Question Type:** **MultipleChoice**

Exhibit.



Quarantine Endpoint by EMS

Playbook to quarantine endpoint by EMS connector

Which statement is true about the FortiAnalyzer playbook configuration shown in the exhibit?

## Options:

A- The playbook is run on a configured schedule

B- The playbook is run when an incident is created that matches the filters.

C- The playbook is run when an event is created that matches the filters

D- The playbook is manually started by an administrator

D- The playbook is manually started by an administrator: The 'ON DEMAND' trigger in the playbook suggests that it is initiated manually, as opposed to being automated or scheduled. This typically means that an administrator decides when to run the playbook based on specific needs or incidents.

## Answer:

D, D

## Explanation:

The FortiAnalyzer playbook configuration shown in the exhibit indicates that:

# Question 11

**Question Type: MultipleChoice**

What are two functions of NGFW in a ZTA deployment? (Choose two.)

## Options:

**A-** Acts as segmentation gateway

**B-** Endpoint vulnerability management

**C-** Device discovery and profiling

**D-** Packet Inspection

## Answer:

A, C

## Explanation:

NGFW stands for Next-Generation Firewall, which is a network security device that provides advanced features beyond the traditional firewall, such as application awareness, identity awareness, threat prevention, and integration with other security tools. ZTA stands for Zero Trust Architecture, which is a security model that requires strict verification of the identity and context of every request before granting access to network resources. ZTA assumes that no device or user can be trusted by default, even if they are connected to a corporate network or have been previously verified.

In a ZTA deployment, NGFW can perform two functions:

Acts as segmentation gateway: NGFW can act as a segmentation gateway, which is a device that separates different segments of the network based on security policies and rules. Segmentation can help isolate and protect sensitive data and applications from unauthorized or malicious access, as well as reduce the attack surface and contain the impact of a breach. NGFW can enforce granular segmentation policies based on the identity and context of the devices and users, as well as the applications and services they are accessing. NGFW can also integrate with other segmentation tools, such as software-defined networking (SDN) and microsegmentation, to provide a consistent and dynamic segmentation across the network.

Device discovery and profiling: NGFW can also perform device discovery and profiling, which are processes that identify and classify the devices that are connected to the network, as well as their attributes and behaviors. Device discovery and profiling can help NGFW to apply the appropriate security policies and rules based on the device type, role, location, health, and activity. Device discovery and profiling can also help NGFW to detect and respond to anomalous or malicious devices that may pose a threat to the network.

: What is a Next-Generation Firewall (NGFW)? | Fortinet : What is Zero Trust Network Access (ZTNA)? | Fortinet :Zero Trust Architecture Explained: A Step-by-Step Approach:The Most Common NGFW Deployment Scenarios:Sample Configuration for Post vWAN Deployment