PassQueen
a.k.a dumpsqueen.com

NSE5_FCT-7.0 NSE 5 - FortiClient EMS 7.0

Fortinet NSE5_FCT-7.0

Version Demo

Total Demo Questions: 7

Total Premium Questions: 70

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Deployment and Configuration	22
Topic 2, Security Fabric Integration	11
Topic 3, Endpoint Security	21
Topic 4, Zero Trust Network Access (ZTNA)	15
Topic 5, Monitoring and Troubleshooting	1
Total	70

QUESTION NO: 1

Refer to the exhibit.

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:

The administrator must resolve the XML syntax error. FortiClient validates an imported XML configuration as structured XML before it can process the contained configuration settings. XML is case-sensitive and must be well formed: every opening tag requires a matching closing tag, elements must be correctly nested, attribute values must be quoted, and the document must

contain only valid XML characters. A manual edit that leaves an unmatched tag, malformed element, or invalid character causes the XML parser to reject the file during restoration. The administrator should therefore compare the edited section with the original exported configuration, correct the malformed XML, and validate the document with an XML-aware editor before importing it again. This preserves the intended FortiClient settings while ensuring that the file can be parsed successfully. Fortinet's FortiClient documentation describes configuration backup and restoration procedures in the FortiClient Administration Guide. General XML well-formedness requirements are defined by the W3C XML specification.

QUESTION NO: 2

Which two actions are required on FortiGate to use FortiClient EMS endpoint tags in access-control policies? (Choose two.)

A. Configure a FortiClient EMS Fabric connector

B. Trust the FortiClient EMS root CA certificate

C. Install FortiClient on FortiGate

D. Configure FortiGate as a FortiClient license server

ANSWER: A B

Explanation:

FortiGate must be configured with a FortiClient EMS Fabric connector so that it can communicate with EMS and retrieve authorized endpoint information. The FortiClient EMS root CA certificate must also be trusted by FortiGate so that FortiGate can validate the certificate chain used by the EMS deployment.

After the connector is established and endpoint tags are synchronized, the administrator can reference those tags in FortiGate firewall policies or ZTNA rules. Installing FortiClient directly on FortiGate is not possible, and FortiGate does not need to act as a FortiClient license server to consume EMS tags. See the FortiGate 7.0 Administration Guide and the FortiClient EMS 7.0 Administration Guide.

QUESTION NO: 3

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

A. It enforces access control

B. It redirects the client request to the access proxy

C. It defines the access proxy

D. It applies security profiles to protect traffic

ANSWER: B

Explanation:

It redirects the client request to the access proxy is correct. In a FortiGate ZTNA access-proxy deployment, the access proxy is represented on the FortiGate by a virtual IP (VIP). The relevant incoming firewall policy receives traffic addressed to that VIP, matches the client request, and forwards it to the configured access proxy for proxying to the protected application. This policy is therefore the traffic-steering point that connects an external client request with the ZTNA access-proxy service.

After the request reaches the access proxy, FortiGate can evaluate the configured ZTNA access-proxy policy, including the applicable ZTNA rule and endpoint posture information supplied by FortiClient/EMS. This architecture lets FortiGate make application-access decisions based on the authenticated user and device context while publishing the private application through the proxy. Fortinet's basic ZTNA configuration documentation explicitly describes the firewall policy as matching client requests and redirecting them to the access-proxy VIP. See Fortinet: Basic ZTNA configuration and FortiGate Administration Guide: ZTNA access proxy.

QUESTION NO: 4

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 shares endpoint device-status information through ZTNA telemetry. Installed on the managed endpoint, FortiClient continuously evaluates the endpoint posture defined by its EMS profile, such as operating-system status, antivirus status, vulnerability findings, running processes, and other security-relevant compliance signals. It sends this telemetry to FortiClient EMS, which uses the information to determine the endpoint's current ZTNA tag assignment and security posture. EMS can then synchronize relevant endpoint and tag information with FortiGate for use in ZTNA access policy decisions. This continuous posture sharing is fundamental to ZTNA because access can be evaluated using the device's current state rather than relying only on network location or a one-time authentication event. Fortinet documentation describes telemetry as the communication mechanism through which FortiClient provides endpoint information to EMS and supports dynamic ZTNA tagging. See the FortiClient EMS Administration Guide and Fortinet's ZTNA administration documentation.

QUESTION NO: 5

Which two web-filtering methods can an administrator configure in a FortiClient endpoint profile? (Choose two.)

A. FortiGuard site categories

B. Web exclusion list

C. FortiGate routing table

D. IPsec phase 1 proposal

ANSWER: A B

Explanation:

FortiClient web filtering can use FortiGuard site categories to apply actions according to the category assigned to a website. This enables administrators to control broad groups of websites, such as categories associated with security risk or unacceptable-use requirements.

An administrator can also configure a web exclusion list to apply actions to specifically identified websites or URL patterns. This is useful when a policy must allow, block, or otherwise control a particular site independently of its category. See the FortiClient EMS 7.0 Administration Guide.

QUESTION NO: 6

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

A. L2TP

B. PPTP

C. IPSec

D. SSL VPN

ANSWER: C D

Explanation:

FortiClient for Windows provides command-line functionality that allows an endpoint user to initiate both IPsec VPN and SSL VPN connections when the applicable connection profiles have been configured. This is useful for scripted deployments, logon procedures, endpoint-management workflows, and support situations where a user or administrator needs to establish a VPN tunnel without interacting with the full graphical interface. The FortiClient command-line interface can select a configured VPN connection and perform connection actions, with authentication handled according to the profile configuration and any required credentials or multifactor-authentication flow. IPsec VPN is supported as a FortiClient remote-access VPN technology, using IPsec tunnel and authentication settings supplied through the client profile. SSL VPN is likewise a FortiClient remote-access technology and can be initiated through the client's command-line capabilities when an SSL VPN profile is available. Fortinet's FortiClient Administration Guide documents Windows client administration and VPN functionality, including command-line-related configuration and operation. Review the FortiClient 7.0 Administration Guide and Fortinet's FortiClient 7.0 documentation portal for the command syntax and version-specific VPN requirements.

QUESTION NO: 7

An administrator wants to simplify remote access without asking users to provide user credentials.

Which access control method provides this solution"?

A. SSL VPN

B. ZTNA full mode

C. L2TP

D. ZTNA IP/MAC filtering mode

ANSWER: D

Explanation:

ZTNA IP/MAC filtering mode provides the appropriate simplified access-control approach because it makes an access decision using the endpoint's network identity, specifically its source IP address and MAC address, rather than requiring an interactive user sign-in. This is useful for managed or known devices in environments where administrators need straightforward remote-access enforcement but do not want users repeatedly prompted to enter credentials. The administrator defines permitted IP/MAC information in the relevant ZTNA policy configuration, and traffic from matching endpoints can be allowed to reach the protected resource. This method is intended for cases in which device or network location identification is sufficient for the required access workflow. It can therefore reduce user friction while retaining an explicit policy-based restriction on which endpoints may connect. Fortinet documents ZTNA configuration and policy concepts in the FortiClient EMS Administration Guide. Related ZTNA access-control and proxy-policy configuration is documented in the FortiGate Administration Guide.