



Vendor: Fortinet

Exam Code: FCSS_EFW_AD-7.4

Exam Name: FCSS - Enterprise Firewall 7.4 Administrator

Version: DEMO

QUESTION 1

A company that acquired multiple branches across different countries needs to install new FortiGate devices on each of those branches. However, the IT staff lacks sufficient knowledge to implement the initial configuration on the FortiGate devices.

Which three approaches can the company take to successfully deploy advanced initial configurations on remote branches? (Choose three.)

- A. Use metadata variables to dynamically assign values according to each FortiGate device.
- B. Use provisioning templates and install configuration settings at the device layer.
- C. Use the Global ADOM to deploy global object configurations to each FortiGate device.
- D. Apply Jinja in the FortiManager scripts for large-scale and advanced deployments.
- E. Add FortiGate devices on FortiManager as model devices, and use ZTP or LTP to connect to FortiGate devices.

Answer: ABE

QUESTION 2

An administrator is checking an enterprise network and sees a suspicious packet with the MAC address e0:23:ff:fc:00:86.

What two conclusions can the administrator draw? (Choose two.)

- A. The suspicious packet is related to a cluster that has VDOMs enabled.
- B. The network includes FortiGate devices configured with the FGSP protocol.
- C. The suspicious packet is related to a cluster with a group-id value lower than 255.
- D. The suspicious packet corresponds to port 7 on a FortiGate device.

Answer: AC

QUESTION 3

A company's guest internet policy, operating in proxy mode, blocks access to Artificial Intelligence Technology sites using FortiGuard. However, a guest user accessed a page in this category using port 8443.

Which configuration changes are required for FortiGate to analyze HTTPS traffic on nonstandard ports like 8443 when full SSL inspection is active in the guest policy?

- A. Add a URL wildcard domain to the website CA certificate and use it in the SSL/SSH Inspection Profile.
- B. In the Protocol Port Mapping section of the SSL/SSH Inspection Profile, enter 443, 8443 to analyze both standard (443) and non-standard (8443) HTTPS ports.
- C. To analyze nonstandard ports in web filter profiles, use TLSv1.3 in the SSL/SSH Inspection Profile.
- D. Administrators can block traffic on nonstandard ports by enabling the SNI check in the SSL/SSH Inspection Profile.

Answer: B

QUESTION 4

An administrator needs to install an IPS profile without triggering false positives that can impact applications and cause problems with the user's normal traffic flow.

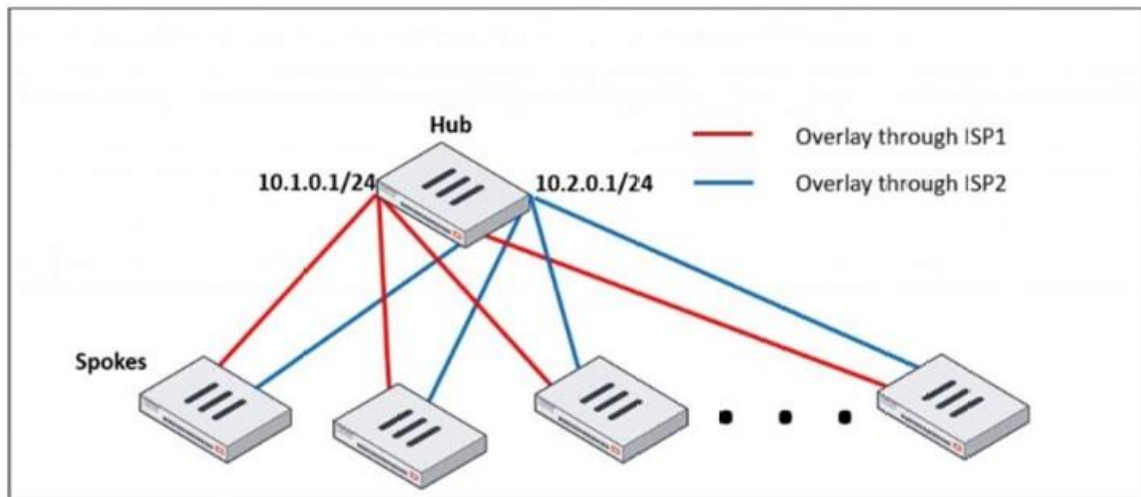
Which action can the administrator take to prevent false positives on IPS analysis?

- A. Use the IPS profile extension to select an operating system, protocol, and application for all the network internal services and users to prevent false positives.
- B. Enable Scan Outgoing Connections to avoid clicking suspicious links or attachments that can deliver botnet malware and create false positives.
- C. Use an IPS profile with action monitor, however, the administrator must be aware that this can compromise network integrity.
- D. Install missing or expired SSL/TLS certificates on the client PC to prevent expected false positives.

Answer: A

QUESTION 5

Refer to the exhibit, which shows a hub and spokes deployment.



An administrator is deploying several spokes, including the BGP configuration for the spokes to connect to the hub.

Which two commands allow the administrator to minimize the configuration? (Choose two.)

- A. neighbor-group
- B. route-reflector-client
- C. neighbor-range
- D. ibgp-enforce-multihop

Answer: AC

QUESTION 6

Why does the ISDB block layers 3 and 4 of the OSI model when applying content filtering? (Choose two.)

- A. FortiGate has a predefined list of all IPs and ports for specific applications downloaded from FortiGuard.
- B. The ISDB blocks the IP addresses and ports of an application predefined by FortiGuard.
- C. The ISDB works in proxy mode, allowing the analysis of packets in layers 3 and 4 of the OSI model.
- D. The ISDB limits access by URL and domain.

Answer: AB

QUESTION 7

Refer to the exhibits. The Administrators section of a root FortiGate device and the Security Fabric Settings section of a downstream FortiGate device are shown.

Root FortiGate - System Administrator configuration

System Administrator 2	
admin	super_admin
AdminSSO	super_admin_readonly

Downstream FortiGate - Security Fabric settings

Security Fabric role	<input type="radio"/> Standalone <input type="radio"/> Serve as Fabric Root <input checked="" type="radio"/> Join Existing Fabric
Allow other Security Fabric devices to join	<input checked="" type="checkbox"/> <div> port1 × </div> <div>+</div>
Upstream FortiGate IP/FQDN	10.1.0.254
Allow downstream device REST API access	<input type="checkbox"/>
SAML Single Sign-On	<input checked="" type="radio"/> Auto <input type="radio"/> Manual <div>Advanced Options</div>
Mode	<div>Service Provider (SP)</div> <input checked="" type="radio"/> Normal <input type="radio"/> Single Sign-On
Default login page	
Default admin profile	super_admin_readonly
Management IP/FQDN	<input type="radio"/> Use WAN IP <input checked="" type="radio"/> Specify <div>10.1.0.100</div>
Management port	<input type="radio"/> Use Admin Port <input checked="" type="radio"/> Specify <div>443</div>

When prompted to sign in with Security Fabric in the downstream FortiGate device, a user enters the AdminSSO credentials.

What is the next status for the user?

- A. The user is prompted to create an SSO administrator account for AdminSSO.
- B. The user receives an authentication failure message.
- C. The user accesses the downstream FortiGate with super_admin_readonly privileges.
- D. The user accesses the downstream FortiGate with super_admin privileges.

Answer: C

QUESTION 8

A user reports that their computer was infected with malware after accessing a secured HTTPS website. However, when the administrator checks the FortiGate logs, they do not see that the website was detected as insecure despite having an SSL certificate and correct profiles applied on the policy.

How can an administrator ensure that FortiGate can analyze encrypted HTTPS traffic on a website?

- A. The administrator must enable reputable websites to allow only SSL/TLS websites rated by FortiGuard web filter.
- B. The administrator must enable URL extraction from SNI on the SSL certificate inspection to ensure the TLS three-way handshake is correctly analyzed by FortiGate.
- C. The administrator must enable DNS over TLS to protect against fake Server Name Indication (SNI) that cannot be analyzed in common DNS requests on HTTPS websites.
- D. The administrator must enable full SSL inspection in the SSL/SSH Inspection Profile to decrypt packets and ensure they are analyzed as expected.

Answer: D