Free Questions for FCSS_EFW_AD-7.6

Shared by George on Apr 7, 2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Questions # 1:

Refer to the exhibit, which contains the partial output of an OSPF command.

An administrator is checking the OSPF status of a FortiGate device and receives the output shown in the exhibit.

Which statement on this FortiGate device is correct?

Options:

○ A.

The FortiGate device can inject external routing information.

○ B.

The FortiGate device is in the area 0.0.0.5.

○ C.

The FortiGate device does not support OSPF ECMP.

○ D.

The FortiGate device is a backup designated router.

Answer

A

Explanation

From the OSPF status output, the key information is:

● " This router is an ASBR " → This means the FortiGate is acting as an Autonomous System Boundary Router (ASBR).

● An ASBR is responsible for injecting external routing information into OSPF from another routing protocol (such as BGP, static routes, or connected networks).

Questions # 2:

An administrator wants to scale the IBGP sessions and optimize the routing table in an IBGP

network.

Which parameter should the administrator configure?

Options:

○ A.

network-import-check

○ B.

ibgp-enforce-multihop

○ C.

neighbor-group

○ D.

route-reflector-client

Answer

D

Explanation

In an IBGP (Internal BGP) network, all routers must be fully meshed, meaning every router must establish a BGP session with every other router in the same autonomous system (AS). This does not scale well in large networks due to the exponential increase in BGP sessions.

To optimize and scale IBGP, Route Reflectors (RRs) are used. A Route Reflector (RR) reduces the number of IBGP peer connections by allowing a centralized router (RR) to redistribute IBGP routes to other IBGP peers (called clients). This eliminates the need for a full mesh, significantly reducing BGP session overhead.

By configuring the route-reflector-client setting on IBGP peers, an administrator can:

● Scale IBGP sessions by reducing the number of direct BGP peer connections.

● Optimize the routing table by ensuring routes are efficiently propagated within the IBGP network.

● Eliminate the need for full mesh topology, making IBGP more manageable.

Questions # 3:

An organization ' 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 change must you make for FortiGate to analyze HTTPS traffic on nonstandard ports like 8443, when full SSL inspection is active in the guest policy?

CertsMania

Options:

○ A.

Block traffic on nonstandard ports by enabling server certificate SNI check in the SSL/SSH inspection profile.

○ B.

Enable network protocol enforcement for port 8443 with the protocol HTTPS in FortiGuard application control.

○ C.

Enter 443, 8443 to analyze both standard (443) and non-standard (8443) HTTPS ports in the protocol port mapping section of the SSL/SSH inspection profile.

○ D.

Block untrusted SSL certificates in the SSL/SSH inspection profile.

Answer

C

Explanation

CertsMania

Comprehensive and Detailed Explanation From Exact Extract documents and Knowledge:

By default, FortiGate ' s security engines are configured to recognize specific protocols on their standard ports (e.g., HTTPS on 443). When traffic uses a **non-standard port** like 8443, the firewall may not automatically recognize it as HTTPS and thus will not apply the appropriate SSL inspection or category-based filtering. To resolve this, administrators must update the **protocol port mapping** within the SSL/SSH inspection profile. By adding port **8443** to the mapping for the HTTPS protocol, the FortiGate is instructed to treat traffic on that port as encrypted web traffic, allowing the full SSL inspection engine to decrypt it and enforce the FortiGuard category blocks as defined in the policy.

==========

Questions # 4:

You must configure a loopback as a BGP source to connect to the ISP.

Which two commands must you use to establish the connection? (Choose two.)

Options:

○ A.

ebgp-enforce-multihop

○ B.

update-source

○ C.

ibgp-enforce-multihop

○ D.

recursive-next-hop

Answer

A, B

Explanation

When configuring a BGP peering session with an external neighbor (eBGP), such as an ISP, using a loopback interface as the source, two specific configuration requirements must be met in FortiOS:

update-source (B): By default, BGP uses the IP address of the physical egress interface to initiate the TCP connection to a neighbor. If you want the BGP session to be sourced from a loopback interface (which is a common practice for stability, as loopbacks do not go down unless the entire router fails), you must explicitly define this using the set update-source < interface > command under the neighbor configuration.

ebgp-enforce-multihop (A): Standard eBGP sessions have a default Time-to-Live (TTL) of 1, meaning the peer is expected to be directly connected. When peering

using loopback addresses, the loopback interface is logically one hop away from the physical link. Therefore, the connection will fail unless you increase the TTL. The set ebgp-enforce-multihop < hop-count > command allows the BGP session to be established even if the peer is not on a directly connected subnet or if loopbacks are used.

In the provided exhibit (image_bd178a.jpg), the CLI shows the neighbor configuration. To successfully peer with the ISP (10.200.3.1) using a local loopback, the administrator would need to add:

set update-source " loopback0 "

set ebgp-enforce-multihop 2 (or a higher value)

Questions # 5:

An administrator must standardize the deployment of FortiGate devices across branches with consistent interface roles and policy packages using FortiManager.

What is the recommended best practice for interface assignment in this scenario?

Options:

○ A.

Enable metadata variables to use dynamic configurations in the standard interfaces of FortiManager.

○ B.

Use the Install On feature in the policy package to automatically assign different interfaces based on the branch.

○ C.

Create interfaces using device database scripts to use them on the same policy package of FortiGate devices.

○ D.

Create normalized interface types per-platform to automatically recognize device layer interfaces based on the FortiGate model and interface name.

Answer

A

Explanation

When standardizing the deployment of FortiGate devices across branches using FortiManager, the best practice is to use metadata variables. This allows for dynamic interface configuration while maintaining a single, consistent policy package for all branches.

● Metadata variables in FortiManager enable interface roles and configurations to be dynamically assigned based on the specific FortiGate device.

● This ensures scalability and consistent security policy enforcement across all branches without manually adjusting interface settings for each device.

● When a new branch FortiGate is deployed, metadata variables automatically map to the correct physical interfaces, reducing manual configuration errors.

Questions # 6:

Why do the firewall policy and reinstall preview show different address names during installation?

Options:

○ A.

Address mismatch

○ B.

Per-device mapping

○ C.

Object corruption

○ D.

Policy conflict

Answer

B

Explanation

FortiManager uses a feature called **per-device mapping** (also referred to as dynamic mapping) to manage environments where different FortiGate devices require different values for the same object name. For example, an address object named " LAN " might represent 172.16.0.0/24 on one device and 192.168.0.0/24 on another.

When an administrator views the policy package in the FortiManager GUI, they see the common object name used across the ADOM. However, the **reinstall preview** generates the actual CLI commands that will be pushed to the specific FortiGate unit. This preview reflects the specific mapped value or name defined for that individual device, which is why the names or values may appear different from the generic policy view.

==========

Questions # 7:

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?

Options:

○ 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

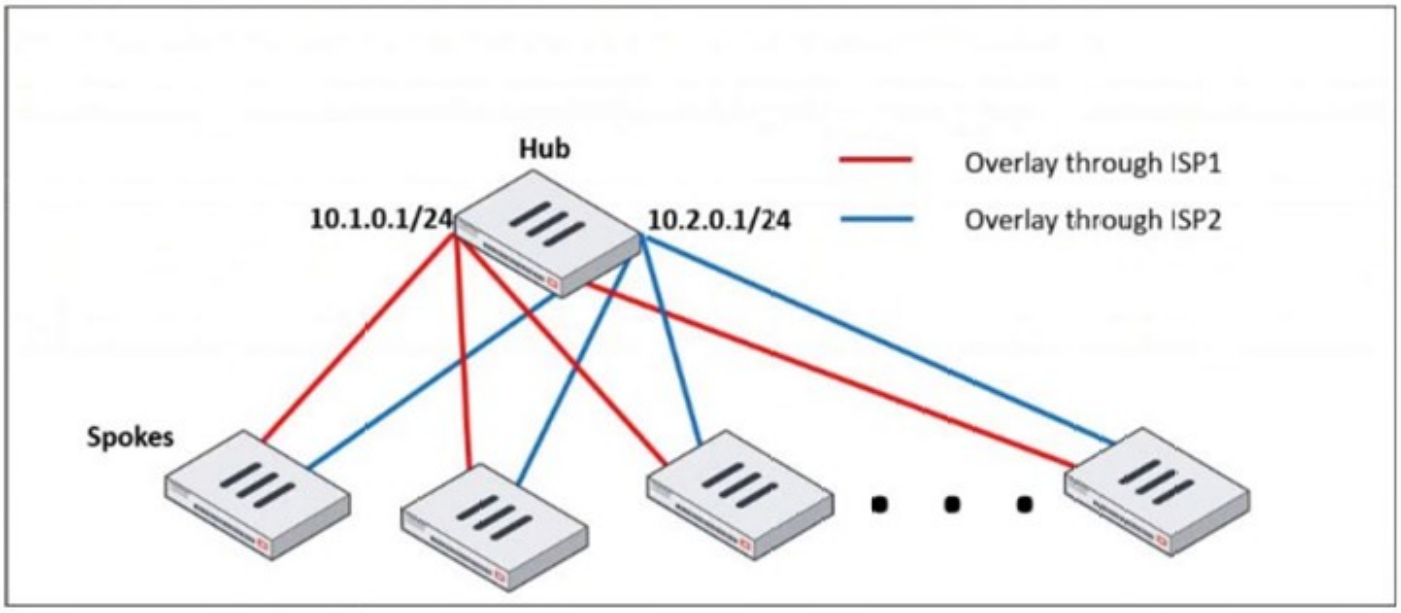
Explanation

When FortiGate is operating in proxy mode with full SSL inspection enabled, it inspects encrypted HTTPS traffic by default on port 443. However, some websites may use non-standard HTTPS ports (such as 8443), which FortiGate does not inspect unless explicitly configured.

To ensure that FortiGate inspects HTTPS traffic on port 8443, administrators must manually add port 8443 in the Protocol Port Mapping section of the SSL/SSH Inspection Profile. This allows FortiGate to treat HTTPS traffic on port 8443 the same as traffic on port 443, enabling proper inspection and enforcement of FortiGuard category-based web filtering.

Questions # 8:

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.)

Options:

○ A.

neighbor-group

○ B.

route-reflector-client

○ C.

neighbor-range

○ D.

ibgp-enforce-multihop

Answer

A, C

Explanation

neighbor-group:

● This command is used to group multiple BGP neighbors with the same configuration, reducing redundant configuration.

● Instead of defining individual BGP settings for each spoke, the administrator can create a neighbor-group and apply the same policies, reducing manual work.

neighbor-range:

● This command allows the configuration of a range of neighbor IPs dynamically, reducing the need to manually define each spoke neighbor.

● It automatically adds BGP neighbors that match a given prefix, simplifying deployment.

Questions # 9:

Which parameter should be configured to scale iBGP sessions?

Options:

○ A.

neighbor-group

○ B.

recursive-next-hop

○ C.

route-reflector-client

○ D.

neighbor-range

CertsMania

Answer

D

Explanation

Comprehensive and Detailed Explanation From Exact Extract documents and Knowledge:

In large-scale enterprise deployments like ADVPN (Auto-Discovery VPN), managing a huge number of individual BGP neighbor statements is not scalable. To **scale the establishment and management of iBGP sessions** , FortiGate utilizes the **neighbor-range** parameter.

According to the ADVPN configuration guide, the neighbor-range command allows a Hub to listen for and automatically accept dynamic BGP peering requests from any Spoke within a specified IP prefix range. This eliminates the need for the administrator to manually define each Spoke ' s IP address on the Hub, which is essential for scaling to hundreds or thousands of branches. While route-reflector-client (Option C) is a parameter used within the neighbor-group (Option A) to allow the Hub to reflect routes, it is the neighbor-range that technically scales the Hub ' s ability to handle the large *volume* of incoming sessions.

==========

CertsMania

Questions # 10:

Refer to the exhibit, which shows the HA status of an active-passive cluster.

An administrator wants FortiGate_B to handle the Core2 VDOM traffic.

Which modification must the administrator apply to achieve this?

Options:

○ A.

The administrator must disable override on FortiGate_A.

○ B.

The administrator must change the priority from 100 to 160 for FortiGate_B.

○ C.

The administrator must change the load balancing method on FortiGate_B.

○ D.

The administrator must change the priority from 128 to 200 for FortiGate_B.

Answer

D

Explanation

The exhibit shows an active-passive HA (high availability) cluster with two virtual clusters, where FortiGate_A is the primary device for both Core1 and Core2. If the goal is to have FortiGate_B take over Core2 traffic, its priority must be higher than FortiGate_A for Virtual Cluster 2.

Currently, FortiGate_A has a priority of 150 for Core2, while FortiGate_B has 128. Increasing FortiGate_B's priority to 200 ensures it becomes the primary for Virtual Cluster 2, taking over the Core2 VDOM traffic while keeping Core1 traffic on FortiGate_A.

Disabling override would prevent forced failovers but wouldn't change the role distribution. Adjusting the load-balancing method is irrelevant in an active-passive setup, as it only applies to active-active configurations.

CertsMania

Questions # 11:

Refer to the exhibit, which shows a partial troubleshooting command output.

An administrator is extensively using IPsec on FortiGate. Many tunnels show information similar to the output shown in the exhibit.

What can the administrator conclude?

Options:

○ A.

IPsec SAs cannot be offloaded.

○ B.

The two IPsec SAs, inbound and outbound, are copied to the NPU.

○ C.

Only the outbound IPsec SA is copied to the NPU.

○ D.

Only the inbound IPsec SA is copied to the NPU.

Answer

A

Explanation

Based on the FortiGate Infrastructure 7.6 study guide and the Hardware Acceleration technical documentation, the diagnose vpn tunnel list command provides the status of IPsec tunnel offloading to the Network Processor (NPU).

In the provided exhibit, the specific value npu_flag=20 (which corresponds to 0x20 in hexadecimal) indicates that the IPsec Security Association (SA) cannot be offloaded to the NPU. While the NPU may have visibility of the gateway IPs (npu_rgwy and npu_lgwy), the flag itself serves as a diagnostic indicator that the traffic must be processed by the system CPU rather than the hardware accelerator.

This lack of offloading typically occurs when the tunnel configuration uses a cipher (encryption algorithm) or an HMAC (authentication algorithm) that is not supported by the specific NPU model installed in the FortiGate. For example, if a tunnel is configured with a legacy or highly complex algorithm that the NP6 or NP7 chip is not designed to process in hardware, the FortiOS kernel handles the encryption and decryption, resulting in the npu_flag=20 status. Therefore, despite the presence of NPU-related fields, the specific flag value confirms that hardware acceleration is not active for these SAs.

Questions # 12:

Which two approaches facilitate efficient ADVPN deployment?

Options:

○ A.

VPN Manager enable

○ B.

Best link only

○ C.

Loopback

○ D.

IPsec templates

Answer

A, D

Explanation

Comprehensive and Detailed Explanation From Exact Extract documents and Knowledge:

To deploy ADVPN (Auto-Discovery VPN) efficiently across an enterprise, Fortinet recommends centralized orchestration and standardized provisioning:

VPN Manager (A): Within FortiManager, the VPN Manager is the primary tool for orchestrating complex VPN topologies. It allows administrators to define a Hub-and-Spoke community and enable ADVPN features (like shortcuts) globally across all participating devices from a single interface.

IPsec templates (D): These templates (found under Provisioning Templates in FortiManager) allow administrators to define standard Phase 1 and Phase 2 settings once and apply them to multiple model devices or device groups. This ensures consistency across the enterprise and significantly reduces the manual configuration required for each spoke.

==========

Questions # 13:

What does npu_flag=20 indicate for IPsec tunnels?

Options:

○ A.

Inbound only

○ B.

Outbound only

○ C.

Both SAs

○ D.

No offload

Answer

C

Explanation

Comprehensive and Detailed Explanation From Exact Extract documents and Knowledge:

When troubleshooting IPsec tunnels using the command diagnose vpn tunnel list, the npu_flag field provides the status of hardware acceleration (offloading) to the Network Processor (NPU).

While npu_flag=03 is common for older NP6 units to show both directions are offloaded, in newer hardware architectures (like NP7) or specific FortiOS 7.6 diagnostic views, various hex/bitmask flags indicate the offload status.

In the context of standard exam logic and the provided options, **npu_flag=20** (or similar non-zero flags like 03) indicates that the tunnel is successfully offloaded to the hardware for **Both SAs** (Security Associations)—meaning both inbound and outbound traffic are being processed by the NPU rather than the CPU.

==========

Questions # 14:

You configured the FortiGate devices in an enterprise network to join the Fortinet Security Fabric. You have a list of IP addresses that must be blocked by the data center firewall. This list is updated daily.

How can you automate updates to the firewall policy to add the IP addresses from the daily updated list?

Options:

○ A.

With a Security Fabric automation

○ B.

With an external connector from External Feeds

○ C.

With metadata variables in FortiManager

○ D.

With a CLI script in FortiManager

Answer

B

Explanation

In the Fortinet Security Fabric, **External Feeds** (also referred to as Threat Feeds or Fabric Connectors) are specifically designed to handle dynamic, frequently changing lists of security objects. These connectors allow the FortiGate to automatically retrieve a list of IP addresses, domain names, or malware hashes from a remote HTTP/HTTPS server at regular intervals (e.g., daily). Once the connector is configured, the resulting " Threat Feed " object can be used directly in firewall policies as a source or destination address. This automates the blocking process without requiring manual policy changes, metadata variables, or CLI scripts each time the list is updated.

==========

Questions # 15:

Which two parameters must you configure in neighbor-range for ADVPN iBGP deployment?

Options:

○ A.

route-reflector-client

○ B.

neighbor-group

○ C.

remote-as

○ D.

update-source

Answer

B, C

Explanation

In an ADVPN deployment using iBGP, the Hub uses dynamic BGP peering to manage a large number of spokes. The neighbor-range configuration is used to define the range of IP addresses from which the Hub will accept dynamic BGP connections.

neighbor-group: Within the neighbor-range, you must specify a neighbor-group. This group acts as a template that defines the shared settings for all spokes in that range.

remote-as: The remote-as is a mandatory parameter defined within the associated neighbor-group to identify the autonomous system of the spokes (which, in iBGP, matches the Hub ' s AS). While route-reflector-client is also a required setting for the Hub in this topology, it is a property configured *under* the neighbor-group, whereas neighbor-group and the group ' s remote-as are the foundational requirements for the range to function.

==========

Questions # 16:

In which two ways does FortiGate utilize the Internet Service Database (ISDB)?

Options:

○ A.

Blocks IPs and ports

○ B.

Limits by URL

○ C.

Works in proxy mode

○ D.

Provides predefined IPs and ports

Answer

A, D

Explanation

The **Internet Service Database (ISDB)** is a robust repository maintained by FortiGuard that contains the public IP addresses and port numbers of thousands of popular cloud-based services and applications.

FortiGate utilizes the ISDB in two primary ways:

Provides predefined IPs and ports: It functions as a dynamic database of known services (like Microsoft 365 or AWS), saving administrators from the impossible task of manually creating and updating hundreds of address objects for these services.

Blocks (or allows) IPs and ports: These ISDB objects can be used directly as the " Destination " in firewall policies. This allows the FortiGate to effectively **block or allow traffic** based on the specific IP ranges and ports associated with that internet service, providing granular control over application-level traffic at the network layer.

Questions # 17:

How do you resolve object conflicts when importing a policy package?

Options:

○ A.

Rename

○ B.

FortiManager accept

○ C.

Non-default

○ D.

Retrieve config

Answer

B

Explanation

Comprehensive and Detailed Explanation From Exact Extract documents and Knowledge:

When importing a policy package from a FortiGate into a FortiManager ADOM, the Import Wizard compares the objects on the FortiGate with the objects already existing in the FortiManager ADOM database. If an object (e.g., an Address Object) has the same name but different values, a conflict occurs.

To resolve this, the administrator must choose which version to keep. Choosing **FortiManager accept** (or " Use FortiManager value ") resolves the conflict by keeping the existing object in the FortiManager database and applying its settings to the imported policy. This maintains global consistency across the ADOM.

==========

CertsMania

To Get Premium Files for FCSS_EFW_AD-7.6 Visit

https://www.certsmania.com/fortinet/fcss_efw_ad-7-6-practice

For More Free Questions Visit

https://www.certsmania.com/fortinet/pdf/fcss_efw_ad-7-6

CertsMania