Download Fortinet FCSS_EFW_AD-7.6 Exam Dumps Free

Shared by Hansen on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An administrator applied a block-all IPS profile for client and server targets to secure the server, but the database team reported the application stopped working immediately after.

How can an administrator apply IPS in a way that ensures it does not disrupt existing applications in the network?

Options:

A- Use an IPS profile with all signatures in monitor mode and verify patterns before blocking.
B- Limit the IPS profile to server targets only to avoid blocking connections from the server to clients.
C- Select flow mode in the IPS profile to accurately analyze application patterns.
D- Set the IPS profile signature action to default to discard all possible false positives.

Answer:

A

Explanation:

Applying an aggressive IPS profile without prior testing can disrupt legitimate applications by incorrectly identifying normal traffic as malicious. To prevent disruptions while still monitoring for threats:

Enable IPS in 'Monitor Mode' first:

This allows FortiGate to log and analyze potential threats without actively blocking traffic.

Administrators can review logs and fine-tune IPS signatures to minimize false positives before switching to blocking mode.

Verify and adjust signature patterns:

Some signatures might trigger unnecessary blocks for legitimate application traffic.

By analyzing logs, administrators can disable or modify specific rules causing false positives.

Question 2

Question Type: MultipleChoice

To secure your enterprise network traffic, which step does FortiGate perform first, when handling the first packets of a session? (Select one answer)

Options:

A- Installation of the session key in the network processor (NP)
B- Decryption
C- A reverse path forwarding (RPF) check
D- IP integrity header checking

Answer:

D

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Enterprise Firewall 7.6 Administrator documents:

Based on the FortiOS 7.6 Administration Guide and the Life of a Packet documentation (Parallel Path Processing), the FortiGate follows a specific, hardcoded sequence when processing the first packet of a new session. This process is divided into several stages: Ingress, Kernel, and Egress.

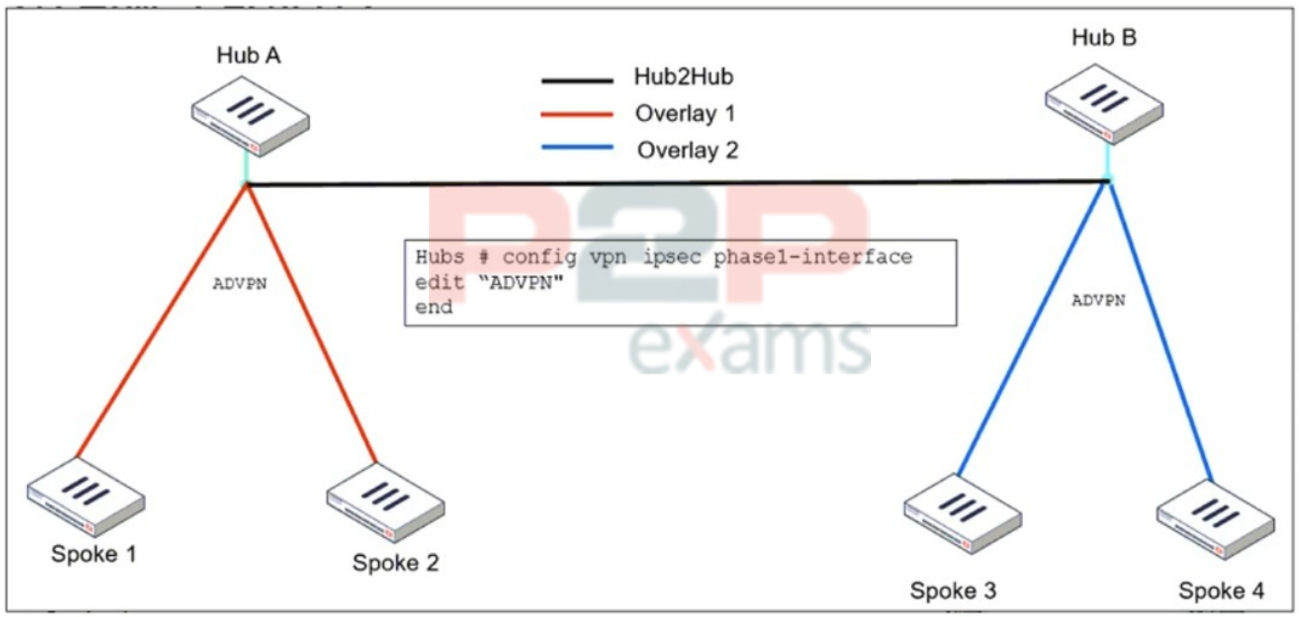
The very first stage is Ingress, where all packets accepted by a network interface are processed by the TCP/IP stack. Immediately following this, the packet must pass through IP integrity header checking. This step involves reading the packet headers to verify that the packet is a valid protocol (TCP, UDP, ICMP, etc.) and that the header length is correct. This sanity check is performed before any other security functions, such as decryption (which occurs later in the Ingress stage) or the Reverse Path Forwarding (RPF) check (which occurs even later during the Routing step in the Kernel stage).

Installation of the session key (Option A) only occurs after the packet has matched a firewall policy and the session has been fully established and offloaded to the NPU. Therefore, IP integrity header checking is the absolute first security-related validation performed on an incoming packet.

Question 3

Question Type: MultipleChoice

Refer to the exhibit, which shows the ADVPN IPsec interface representing the VPN IPsec phase 1 from Hub A to Spoke 1 and Spoke 2, and from Hub to Spoke 3 and Spoke 4.



An administrator must configure an ADVPN using IBGP and EBGP to connect overlay network 1 with 2.

What must the administrator configure in the phase 1 VPN IPsec configuration of the ADVPN tunnels?

Options:

A- set auto-discovery-sender enable and set network-id x
B- set auto-discovery-forwarder enable and set remote-as x
C- set auto-discovery-crossover enable and set enforce-multihop enable
D- set auto-discovery-receiver enable and set npu-offload enable

Answer:

C

Explanation:

When configuring ADVPN (Auto-Discovery VPN) to connect overlay networks across different hubs using IBGP and EBGP, special configurations are required to allow spokes from different overlay networks to dynamically establish tunnels.

set auto-discovery-crossover enable

This allows cross-hub tunnel discovery in an ADVPN deployment where multiple hubs are used.

Since Hub A and Hub B belong to different overlays, enabling crossover discovery ensures that spokes from one overlay can dynamically create direct tunnels to spokes in the other overlay when needed.

set enforce-multihop enable

This setting ensures that BGP peers using loopback interfaces can establish connectivity even if they are not directly connected.

Multihop BGP sessions are required when using loopback addresses as BGP peer sources because the connection might need to traverse multiple routers before reaching the BGP neighbor.

This is especially useful in ADVPN deployments with multiple hubs, where routes might need to cross from one hub to another.

Question 4

Question Type: MultipleChoice

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.

Question 5

Question Type: MultipleChoice

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

```
FortiGate # get router info ospf status
 Routing Process "ospf 0" with ID 0.0.0.5
 Process uptime is 0 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Do not support Restarting
 This router is an ASBR
```

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:

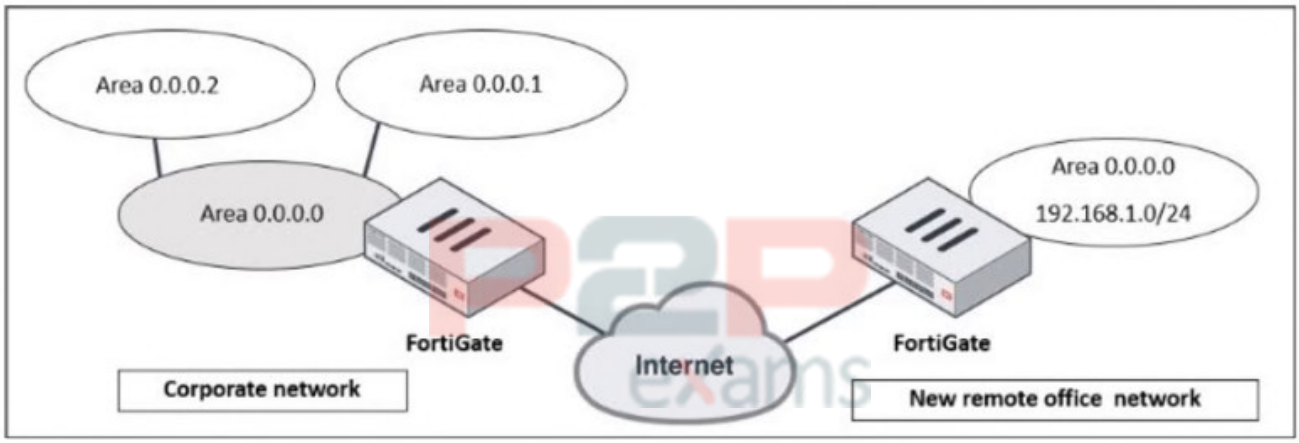
'This router is an ASBR' This means the FortiGate is acting as an Autonomous System Boundary Router (ASBR).

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

Question 6

Question Type: MultipleChoice

Refer to the exhibit, which shows a corporate network and a new remote office network.



An administrator must integrate the new remote office network with the corporate enterprise network.

What must the administrator do to allow routing between the two networks?

Options:

A- The administrator must implement BGP to inject the new remote office network into the

corporate FortiGate device

B- The administrator must configure a static route to the subnet 192.168.l.0/24 on the corporate FortiGate device.

C- The administrator must configure virtual links on both FortiGate devices.

D- The administrator must implement OSPF over IPsec on both FortiGate devices.

Answer:

D

Explanation:

In this scenario, the corporate network and the new remote office network need to communicate over the Internet, which requires a secure and dynamic routing method. Since both networks are using OSPF (Open Shortest Path First) as the routing protocol, the best approach is to establish an OSPF over IPsec VPN to ensure secure and dynamic route propagation.

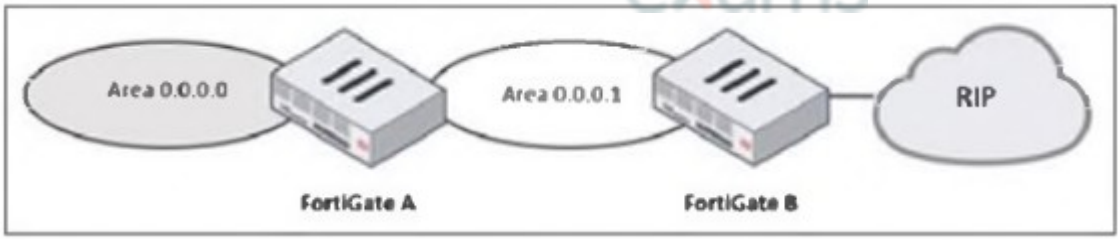
OSPF is already running on the corporate network, and extending it over an IPsec tunnel allows dynamic route exchange between the corporate FortiGate and the remote office FortiGate. IPsec provides encryption for traffic over the Internet, ensuring secure communication. OSPF over IPsec eliminates the need for manual static routes, allowing automatic route updates if networks change.

The new remote office's 192.168.1.0/24 subnet will be advertised dynamically to the corporate network without additional configuration.

Question 7

Question Type: MultipleChoice

Refer to the exhibit, which shows a partial enterprise network.



An administrator would like the area 0.0.0.0 to detect the external network.

What must the administrator configure?

Options:

A- Enable RIP redistribution on FortiGate B.
B- Configure a distribute-route-map-in on FortiGate B.
C- Configure a virtual link between FortiGate A and B.
D- Set the area 0.0.0.l type to stub on FortiGate A and B.

Answer:

A

Explanation:

The diagram shows a multi-area OSPF network where:

FortiGate A is in OSPF Area 0 (Backbone area).

FortiGate B is in OSPF Area 0.0.0.1 and is connected to an RIP network.

To ensure that OSPF Area 0 (0.0.0.0) learns routes from the external RIP network, FortiGate B must redistribute RIP routes into OSPF.

Steps to achieve this:

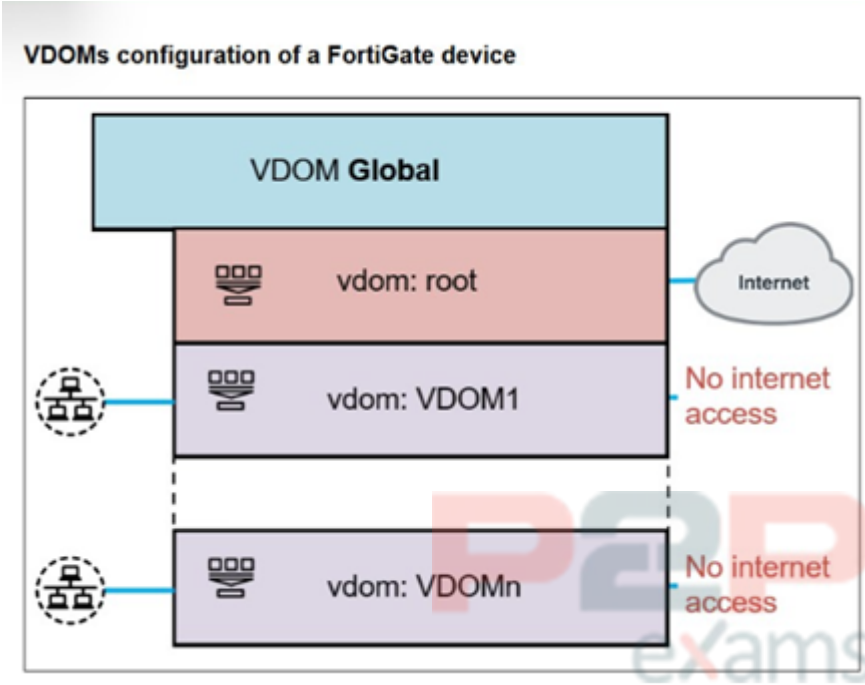
1. Enable route redistribution on FortiGate B to inject RIP-learned routes into OSPF.

2. This allows OSPF Area 0.0.0.1 to forward RIP routes to OSPF Area 0 (0.0.0.0), making the external network visible.

Question 8

Question Type: MultipleChoice

Refer to the exhibit.



A FortiGate segmented into VDOMs is shown. You must ensure effective and accelerated internet access for all of the VDOMs in this enterprise network. How can you achieve this? (Choose one answer)

Options:

A- Connect a physical interface from each VDOM to the root VDOM.
B- Create VDOM links.
C- Configure network processing unit (NPU) vlinks.
D- Create VLANs over network processing unit (NPU) vlinks.

Answer:

C

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of Enterprise Firewall 7.6 Administrator documents:

According to the FortiOS 7.6 Administration Guide and the FortiGate Infrastructure study materials, inter-VDOM communication can be achieved using either software-based VDOM links or hardware-accelerated NPU VDOM links (vlinks).

While standard VDOM links (Option B) allow traffic to pass between VDOMs, they are processed by the system CPU, which can become a bottleneck in high-throughput environments. To ensure accelerated internet access as specified in the requirements, NPU vlinks (Option C) must be used.

NPU vlinks are virtual interfaces created in pairs that allow traffic to be offloaded to the FortiGate's Network Processor (NP6, NP7, etc.), significantly reducing latency and CPU overhead.

In the provided exhibit, the root VDOM has direct internet access, while VDOM1 and VDOMn do not. By configuring NPU vlinks between the non-root VDOMs and the root VDOM, you create a hardware-accelerated path. Traffic from the internal VDOMs is sent through the vlink to the root VDOM, which then forwards it to the Internet. This 'hub-and-spoke' VDOM architecture, powered by NPU acceleration, ensures that all VDOMs share the internet connection without sacrificing performance.

Question 9

Question Type: MultipleChoice

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.