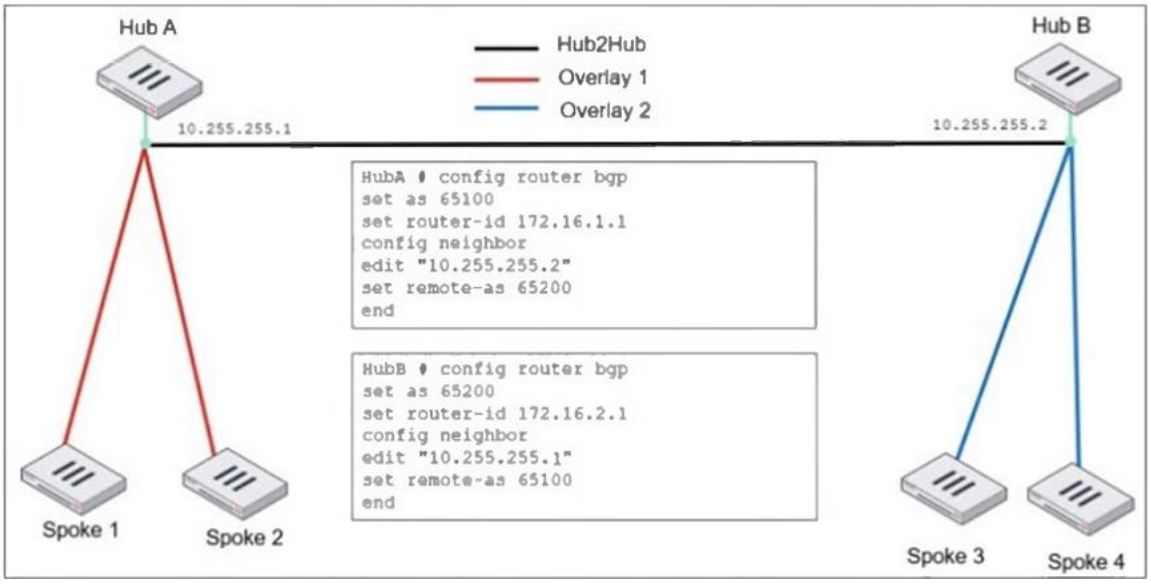
Vendor: Fortinet

Exam Code: FCSS_EFW_AD-7.4

Exam Name: FCSS - Enterprise Firewall 7.4 Administrator

Version: DEMO

QUESTION 1
Refer to the exhibit, which shows an ADVPN network.



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

What two options must the administrator configure in BGP? (Choose two.)

A. set ebgp-enforce-multrhop enable
B. set next-hop-self enable
C. set ibgp-enforce-multihop advpn
D. set attribute-unchanged next-hop

Answer: AB
Explanation:
In this ADVPN (Auto-Discovery VPN) network, there are two hubs (Hub A and Hub B) connected via EBGP, while IBGP is used within each overlay. To ensure proper BGP routing between the overlays, the administrator must configure specific BGP options..

set ebgp-enforce-multihop enable
By default, EBGP requires directly connected neighbors. Since Hub A and Hub B are not directly connected but reach each other over an IPsec tunnel, multihop must be enabled for EBGP sessions to work.

set next-hop-self enable
In IBGP, the next-hop attribute does not change by default. When an IBGP route is advertised from a spoke to another hub or spoke, the next-hop needs to be updated to ensure proper reachability. Enabling next-hop-self forces the BGP speaker to advertise itself as the next-hop, ensuring that all spokes properly reach routes across the overlays.

QUESTION 2
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 ABR
```

An administrator is checking the OSPF status of a FortiGate device and receives the output shown in the exhibit.
What two conclusions can the administrator draw? (Choose two.)

A. The FortiGate device is a backup designated router
B. The FortiGate device is connected to multiple areas
C. The FortiGate device injects external routing information
D. The FortiGate device has OSPF ECMP enabled

Answer: BC
Explanation:
The output of the get router info ospf status command provides key information about the OSPF (Open Shortest Path First) configuration on the FortiGate device.

The FortiGate device is connected to multiple areas
The output states: "This router is an ABR"
ABR (Area Border Router) means the device is connected to multiple OSPF areas and maintains routing information between them.
This confirms that the FortiGate is not just in one area, but at least one backbone area (Area 0) and another OSPF area.

The FortiGate device injects external routing information
The output states: "Supports opaque LSA"
Opaque LSAs (Type 9, 10, and 11) are used in OSPF extensions, including those that support external route injection.
Typically, ABRs or ASBRs (Autonomous System Boundary Routers) inject external routes, allowing routes from other routing protocols (such as BGP or static routes) to be advertised into OSPF.

QUESTION 3
The IT department discovered during the last network migration that all zero phase selectors in phase 2 IPsec configurations impacted network operations. What are two valid approaches to prevent this during future migrations? (Choose two.)

A. Use routing protocols to specify allowed subnets over the tunnel.
B. Configure an IPsec-aggregate to create redundancy between each firewall peer.
C. Clearly indicate to the VPN which segments will be encrypted in the phase two selectors.

D. Configure an IP address on the IPsec interface of each firewall to establish unique peer connections and avoid impacting network operations.

Answer: AC
Explanation:
Zero phase selectors in IPsec Phase 2 mean that no specific traffic selectors (subnets) are defined, allowing any traffic to be encrypted through the VPN tunnel. This can cause unintended traffic forwarding issues and disrupt network operations.
To prevent this from happening during future migrations:
Using routing protocols ensures that only specific subnets are advertised over the tunnel. Dynamic routing (such as OSPF or BGP) helps define which networks should use the tunnel, preventing unintended traffic from being encrypted.
Clearly defining phase 2 selectors avoids the problem of encrypting all traffic by explicitly stating the allowed source and destination subnets. This prevents the tunnel from affecting unrelated network traffic.

QUESTION 4
How will configuring set tcp-mss-sender and set tcp-mss-receiver in a firewall policy affect the size and handling of TCP packets in the network?

A. The maximum segment size permitted in the firewall policy determines whether TCP packets are allowed or denied.
B. Applying commands in a firewall policy determines the largest payload a device can handle in a single TCP segment.
C. The administrator must consider the payload size of the packet and the size of the IP header to configure a correct value in the firewall policy.
D. The TCP packet modifies the packet size only if the size of the packet is less than the one the administrator configured in the firewall policy.

Answer: B
Explanation:
The set tcp-mss-sender and set tcp-mss-receiver commands in a firewall policy allow an administrator to adjust the Maximum Segment Size (MSS) of TCP packets.

This setting controls the largest payload size that a device can handle in a single TCP segment, ensuring that packets do not exceed the allowed MTU (Maximum Transmission Unit) along the network path.
set tcp-mss-sender adjusts the MSS value for outgoing TCP traffic. set tcp-mss-receiver adjusts the MSS value for incoming TCP traffic.

This helps prevent issues with fragmentation and MTU mismatches, improving network performance and avoiding retransmissions.

QUESTION 5
A vulnerability scan report has revealed that a user has generated traffic to the website example.com (10.10.10.10) using a weak SSL/TLS version supported by the HTTPS web server. What can the firewall administrator do to block all outdated SSL/TLS versions on any HTTPS web server to prevent possible attacks on user traffic?

A. Configure the unsupported SSL version and set the minimum allowed SSL version in the HTTPS settings of the SSL/SSH inspection profile.
B. Enable auto-detection of outdated SSL/TLS versions in the SSL/SSH inspection profile to

block vulnerable websites.

C. Install the required certificate in the client's browser or use Active Directory policies to block specific websites as defined in the SSL/SSH inspection profile.
D. Use the latest certificate, Fortinet_SSL_ECDSA256, and replace the CA certificate in the SSL/SSH inspection profile.

Answer: A
Explanation:
The best way to block outdated SSL/TLS versions is to configure the SSL/SSH inspection profile to enforce a minimum SSL/TLS version and disable weak SSL versions. By setting the minimum allowed SSL version in the HTTPS settings of the SSL/SSH inspection profile, FortiGate will: Block any connection using outdated SSL/TLS versions (such as SSLv3, TLS 1.0, or TLS 1.1). Enforce secure communication using only strong SSL/TLS versions (such as TLS 1.2 or TLS 1.3). Protect users from man-in-the-middle (MITM) and downgrade attacks that exploit weak encryption.

QUESTION 6
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?

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 7
An administrator is setting up an ADVPN configuration and wants to ensure that peer IDs are not exposed during VPN establishment.
Which protocol can the administrator use to enhance security?

A. Use IKEv2, which encrypts peer IDs and prevents exposure.
B. Opt for SSL VPN web mode because it does not use peer IDs at all.
C. Choose IKEv1 aggressive mode because it simplifies peer identification.
D. Stick with IKEv1 main mode because it offers better performance.

Answer: A
Explanation:
In ADVPN (Auto-Discovery VPN) configurations, security concerns include protecting peer IDs during VPN establishment. Peer IDs are exchanged in the IKE (Internet Key Exchange) negotiation phase, and their exposure could lead to privacy risks or targeted attacks. IKEv2 encrypts peer IDs, making it more secure compared to IKEv1, where peer IDs can be exposed in plaintext in aggressive mode.
IKEv2 also provides better performance and flexibility while supporting dynamic tunnel establishment in ADVPN.

QUESTION 8
An administrator must minimize CPU and RAM use on a FortiGate firewall while also enabling essential security features, such as web filtering and application control for HTTPS traffic. Which SSL inspection setting helps reduce system load while also enabling security features, such as web filtering and application control for encrypted HTTPS traffic?

A. Use full SSL inspection to thoroughly inspect encrypted payloads.
B. Disable SSL inspection entirely to conserve resources.
C. Configure SSL inspection to handle HTTPS traffic efficiently.
D. Enable SSL certificate inspection mode to perform basic checks without decrypting traffic.

Answer: D
Explanation:
To minimize CPU and RAM usage while still enforcing security features like web filtering and application control, SSL certificate inspection mode is the best choice. SSL certificate inspection allows FortiGate to inspect only the SSL/TLS handshake, including the Server Name Indication (SNI) and certificate details, without decrypting the full encrypted payload. This enables features like web filtering and application control because FortiGate can determine the destination website or application based on SNI and certificate information. It significantly reduces system load compared to full SSL inspection, which requires full decryption and re-encryption of traffic.

QUESTION 9
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?

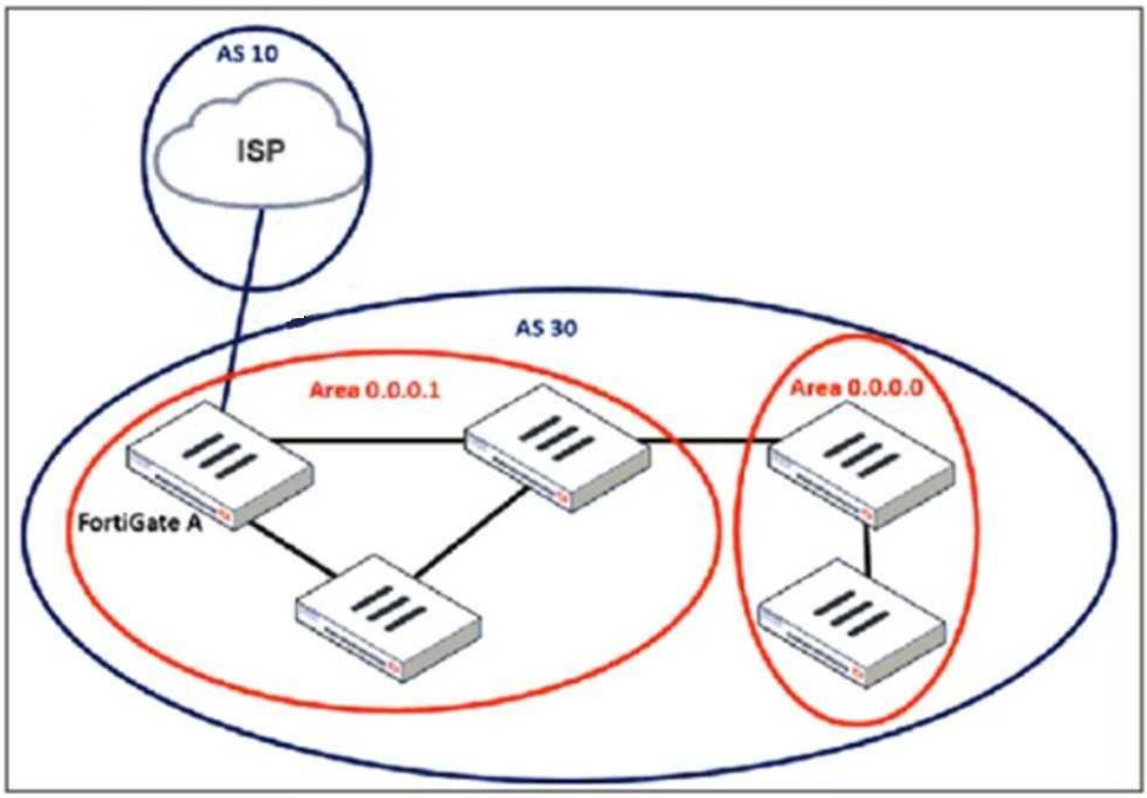
A. Enable metadata variables to use dynamic configurations in the standard interfaces of FortiManager.
B. Use the Install On feature in the policy package to automatically assign different interfaces based on the branch.
C. Create interfaces using device database scripts to use them on the same policy 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 10
Refer to the exhibit, which shows an enterprise network connected to an internet service provider.



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

Which two commands are required to establish the connection? (Choose two.)

A. ebgp-enforce-multihop
B. update-source
C. ibgp-enforce-multihop

D. recursive-next-hop

Answer: AB
Explanation:
When configuring a loopback interface as the BGP source for connecting to an ISP, two important settings must be applied:
1. Enable EBGP Multihop (ebgp-enforce-multihop)
BGP normally expects directly connected neighbors, but since the ISP and FortiGate A are using loopback interfaces, packets will not be sent directly between their physical interfaces. The ebgp-enforce-multihop command allows BGP to form an eBGP peering over multiple hops.

2. Set the Update Source (update-source)
Since FortiGate is using a loopback interface as the source, the update-source command ensures that BGP updates originate from the loopback interface rather than a physical interface. This is essential because BGP peers must match the source IP with the configured neighbor address.

QUESTION 11
What action can be taken on a FortiGate to block traffic using IPS protocol decoders, focusing on network transmission patterns and application signatures?

A. Use the DNS filter to block application signatures and protocol decoders.
B. Use application control to limit non-URL-based software handling.
C. Enable application detection-based SD-WAN rules.
D. Configure a web filter profile in flow mode.

Answer: B
Explanation:
FortiGate's IPS protocol decoders analyze network transmission patterns and application signatures to identify and block malicious traffic. Application Control is the feature that allows FortiGate to detect, classify, and block applications based on their behavior and signatures, even when they do not rely on traditional URLs.
Application Control works alongside IPS protocol decoders to inspect packet payloads and enforce security policies based on recognized application behaviors. It enables granular control over non-URL-based applications such as P2P traffic, VoIP, messaging apps, and other non-web-based protocols that IPS can identify through protocol decoders. IPS and Application Control together can detect evasive or encrypted applications that might bypass traditional firewall rules.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**