

# Fortinet

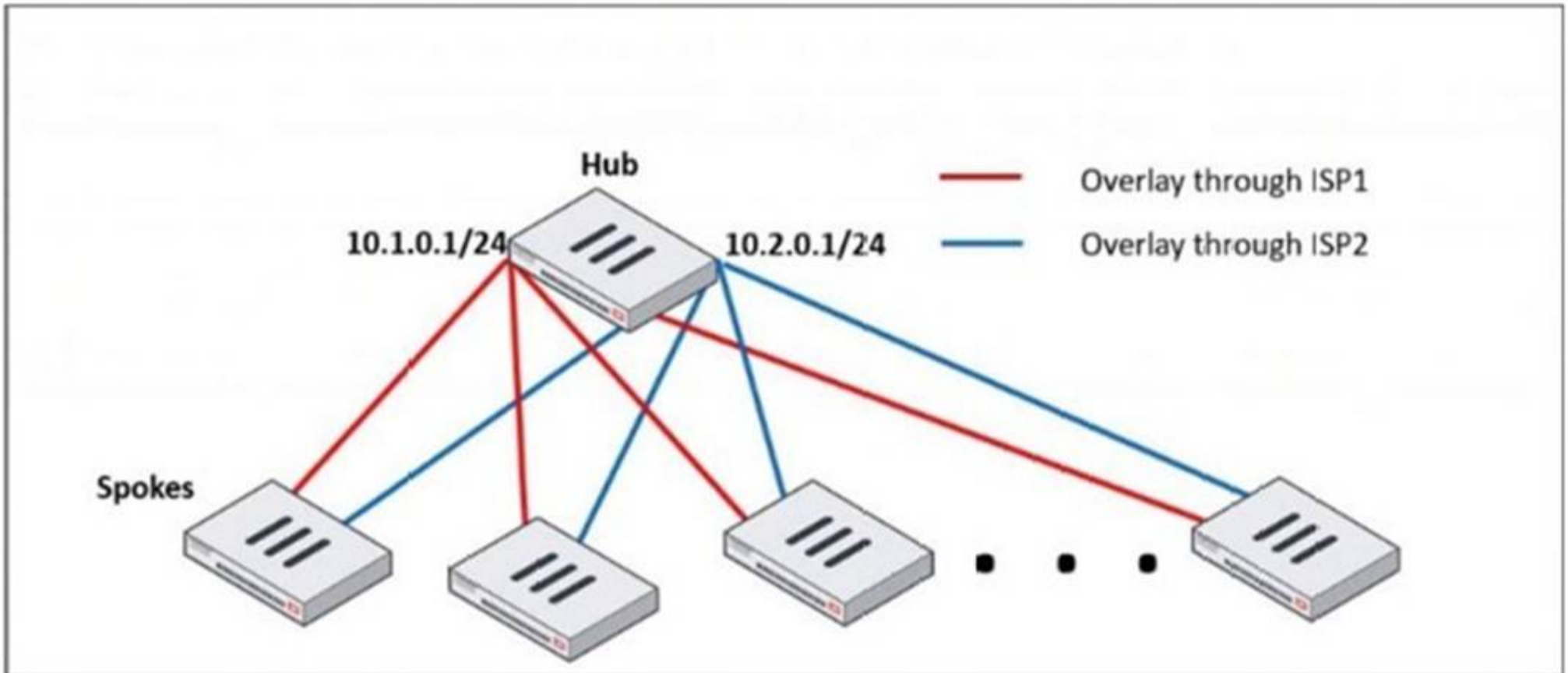
## Exam Questions FCSS\_EFW\_AD-7.6

FCSS - Enterprise Firewall 7.6 Administrator



**NEW QUESTION 1**

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

**NEW QUESTION 2**

Refer to the exhibit, which contains a partial command output.

```
FortiGate # get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 100.65.4.1, remote AS 65300, local AS 65200, external link
BGP version 4, remote router ID 0.0.0.0
BGP state = Idle
Not directly connected EBGP
Last read      , hold time is 180, keepalive interval is 60 seconds
Configured hold time is 180, keepalive interval is 60 seconds
Received 0 messages, 0 notifications, 0 in queue
Sent 0 messages, 0 notifications, 0 in queue
Route refresh request: received 0, sent 0
NLRI treated as withdraw: 0
Minimum time between advertisement runs is 30 seconds
Update source is Loopback
```

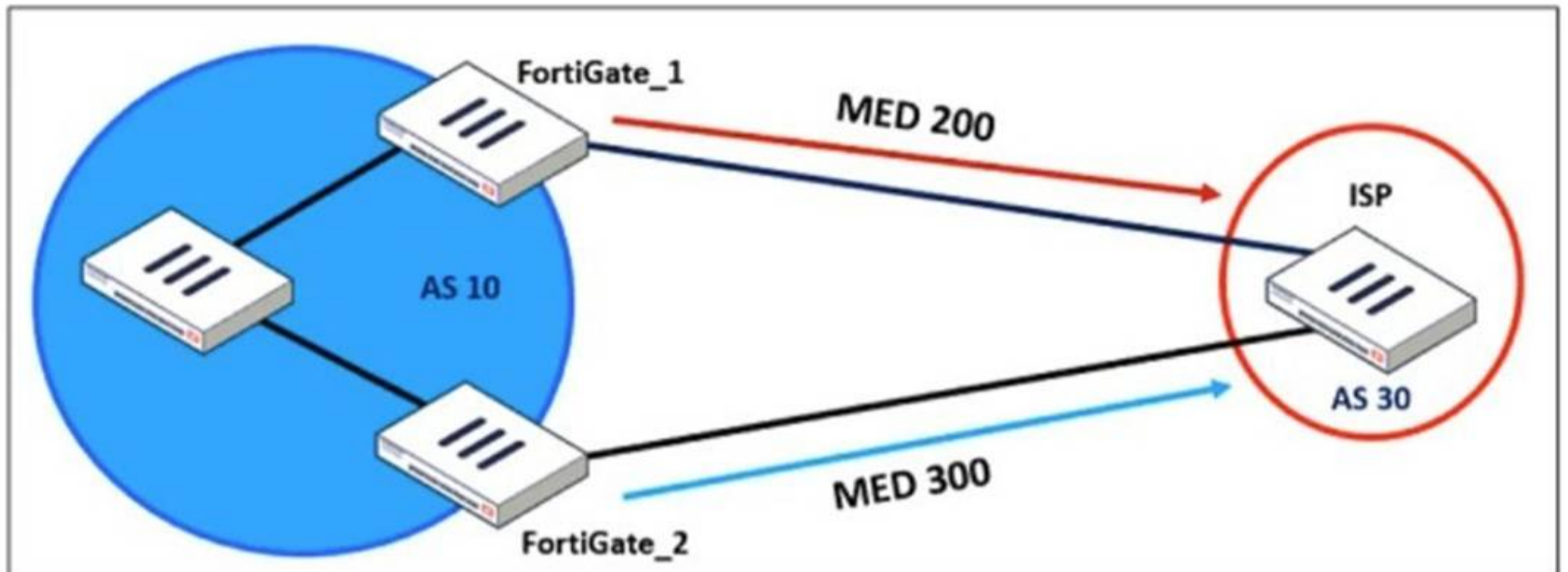
The administrator has configured BGP on FortiGate. The status of this new BGP configuration is shown in the exhibit. What configuration must the administrator consider next?

- A. Configure a static route to 100.65.4.1.
- B. Configure the local AS to 65300.
- C. Contact the remote peer administrator to enable BGP
- D. Enable ebgp-enforce-multihop.

**Answer:** D

**NEW QUESTION 3**

Refer to the exhibit, which shows a network diagram.



An administrator would like to modify the MED value advertised from FortiGate\_1 to a BGP neighbor in the autonomous system 30. What must the administrator configure on FortiGate\_1 to implement this?

- A. route-map-out
- B. network-import-check
- C. prefix-list-out
- D. distribute-list-out

**Answer: A**

**NEW QUESTION 4**

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**

**NEW QUESTION 5**

An administrator received a FortiAnalyzer alert that a 1 disk filled up in a day. Upon investigation, they found thousands of unusual DNS log requests, such as JHCMQK.website.com, with no answers. They later discovered that DNS exfiltration was occurring through both UDP and TLS.

How can the administrator prevent this data theft technique?

- A. Create an inline-CASB to protect against DNS exfiltration.
- B. Configure a File Filter profile to prevent DNS exfiltration.
- C. Enable DNS Filter to protect against DNS exfiltration.
- D. Use an IPS profile and DNS exfiltration-related signatures.

**Answer: D**

**NEW QUESTION 6**

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**

**NEW QUESTION 7**

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

Which parameter should the administrator configure?

- A. network-import-check
- B. ibgp-enforce-multihop
- C. neighbor-group
- D. route-reflector-client

**Answer: D**

**NEW QUESTION 8**

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**

**NEW QUESTION 9**

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**

**NEW QUESTION 10**

A FortiGate device with UTM profiles is reaching the resource limits, and the administrator expects the traffic in the enterprise network to increase. The administrator has received an additional FortiGate of the same model.

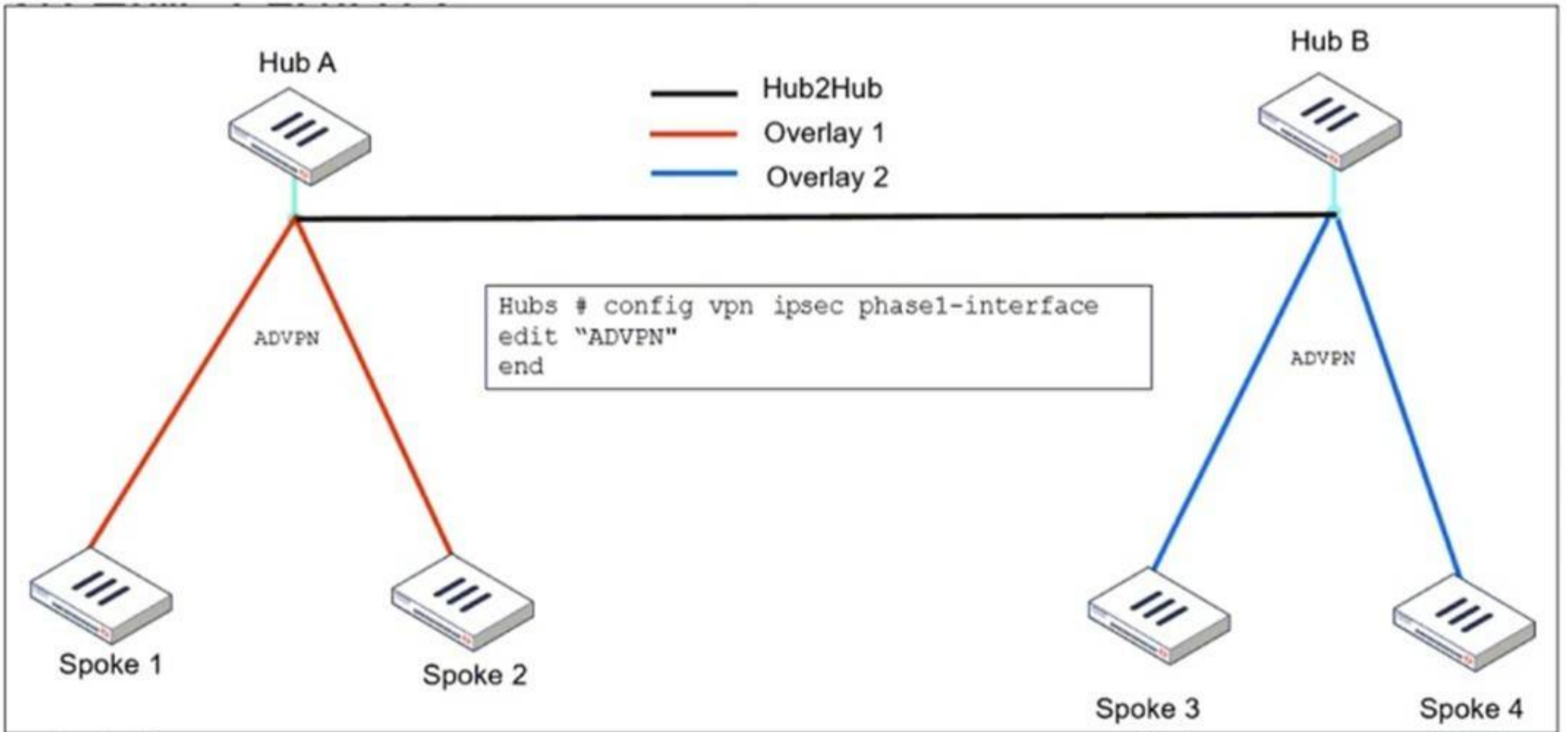
Which two protocols should the administrator use to integrate the additional FortiGate device into this enterprise network? (Choose two.)

- A. FGSP with external load balancers
- B. FGCP in active-active mode and with switches
- C. FGCP in active-passive mode and with VDOM disabled
- D. VRRP with switches

**Answer: AB**

**NEW QUESTION 10**

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?

- 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**

**NEW QUESTION 14**

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**

**NEW QUESTION 16**

Refer to the exhibit, which shows a command output.

```
FortiGate_B # get system session list | grep icmp  
  
FortiGate_B #
```

FortiGate\_A and FortiGate\_B are members of an FGSP cluster in an enterprise network. While testing the cluster using the ping command, the administrator monitors packet loss and found that the session output on FortiGate\_B is as shown in the exhibit. What could be the cause of this output on FortiGate\_B?

- A. The session synchronization is encrypted.
- B. session-pickup-connectionless is set to disable on FortiGate\_B.
- C. FortiGate\_B is configured in passive mode.
- D. FortiGate\_A and FortiGate\_B have the same standalone-group-id value.

**Answer: B**

**NEW QUESTION 20**

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**

**NEW QUESTION 21**

Refer to the exhibit, which shows the FortiGuard Distribution Network of a FortiGate device. FortiGuard Distribution Network on FortiGate

License Information	
Entitlement	Status
Advanced Malware Protection	Licensed (Expiration Date: 2025/11/10)
Attack Surface Security Rating	Licensed (Expiration Date: 2025/11/10)
IoT Detection Definitions	Version 0.00000
Outbreak Package Definitions	Version 5.00036
Security Rating & CIS Compliance	Licensed (Expiration Date: 2025/11/10)
Data Loss Prevention (DLP)	Not Licensed
DLP Signatures	Version 0.00000
Intrusion Prevention	Licensed (Expiration Date: 2025/11/10)
IPS Definitions	Version 28.00821
IPS Engine	Version 7.00539
Malicious URLs	Version 1.00001
Botnet IPs	Version 7.03758
Botnet Domains	Version 3.00847
Operational Technology (OT) Security Service	Licensed (Expiration Date: 2025/11/10)
Web Filtering	Licensed (Expiration Date: 2025/11/10)
Blocked Certificates	Version 1.00487
DNS Filtering	Licensed (Expiration Date: 2025/11/10)
Video Filtering	Licensed (Expiration Date: 2025/11/10)
SD-WAN Network Monitor	Not Licensed
SD-WAN Overlay as a Service	Not Licensed

An administrator is trying to find the web filter database signature on FortiGate to resolve issues with websites not being filtered correctly in a flow-mode web filter profile.

Why is the web filter database version not visible on the GUI, such as with IPS definitions?

- A. The web filter database is stored locally, but the administrator must run over CLI diagnose autoupdate versions.
- B. The web filter database is stored locally on FortiGate, but it is hidden behind the GU
- C. It requires enabling debug mode to make it visible.
- D. The web filter database is not hosted on FortiGate: FortiGate queries FortiGuard or FortiManager for web filter ratings on demand.
- E. The web filter database is only accessible after manual syncing with a valid FDS server using diagnose test update info.

**Answer: C**

**NEW QUESTION 25**

What is the initial step performed by FortiGate when handling the first packets of a session?

- A. Installation of the session key in the network processor (NP)
- B. Data encryption and decryption
- C. Security inspections such as ACL, HPE, and IP integrity header checking
- D. Offloading the packets directly to the content processor (CP)

**Answer: C**

**NEW QUESTION 29**

Refer to the exhibit, which shows a physical topology and a traffic log.



The administrator is checking on FortiAnalyzer traffic from the device with IP address 10.1.10.1, located behind the FortiGate ISFW device. The firewall policy in on the ISFW device does not have UTM enabled and the administrator is surprised to see a log with the action Malware, as shown in the exhibit.

What are the two reasons FortiAnalyzer would display this log? (Choose two.)

- A. Security rating is enabled in ISFW.
- B. ISFW is in a Security Fabric environment.
- C. ISFW is not connected to FortiAnalyzer and must go through NGFW-1.
- D. The firewall policy in NGFW-1 has UTM enabled.

**Answer: BD**

**NEW QUESTION 30**

Refer to the exhibit, which shows a revision history window in the FortiManager device layer.

ID	Date & Time	Name	Created by	Installation	Comments
✓ 10	2024-08-21 14:30:54		script_manager	Retrieved	
9	2024-08-21 14:02:55	AutoUpdate	AutoUpdate	Auto Updated	Autoretrieve merged config
8	2024-06-24 04:52:47	DCFV	admin	Installed	

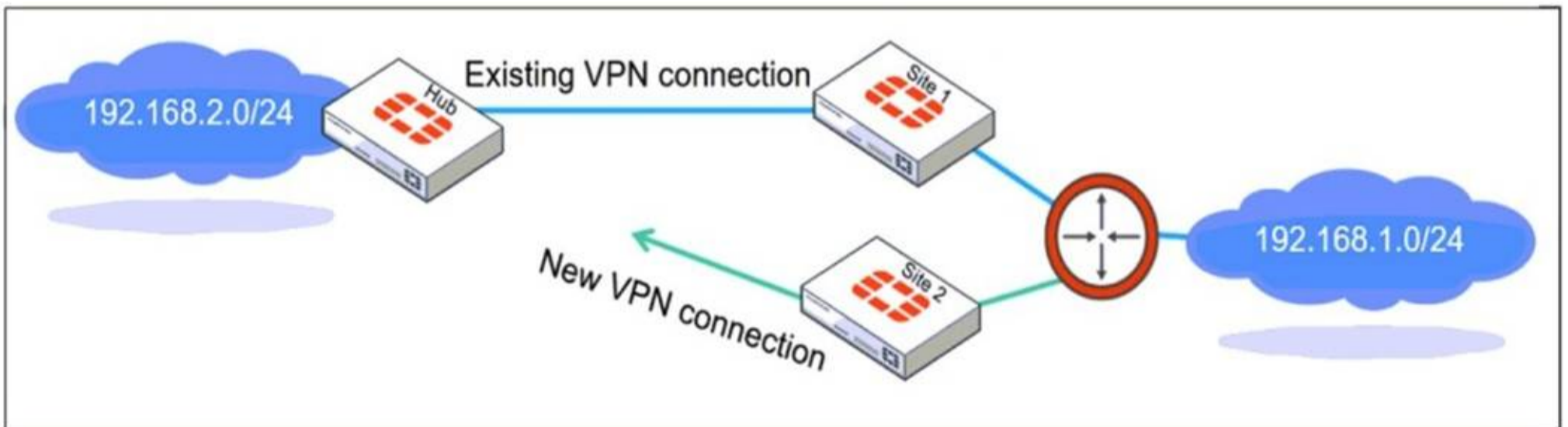
The IT team is trying to identify the administrator responsible for the most recent update in the FortiGate device database. Which conclusion can you draw about this scenario?

- A. This retrieved process was automatically triggered by a Remote FortiGate Directly (via CLI) script.
- B. The user script\_manager is an API user from the Fortinet Developer Network (FDN) retrieving a configuration.
- C. To identify the user who created the event, check it on the Configuration and Installation widget on FortiGate within the FortiManager device layer.
- D. Find the user in the FortiManager system logs and use the type=script command to find the administrator user in the user field.

**Answer: D**

**NEW QUESTION 35**

Refer to the exhibit, which shows a network diagram showing the addition of site 2 with an overlapping network segment to the existing VPN IPsec connection between the hub and site 1.



Which IPsec phase 2 configuration must an administrator make on the FortiGate hub to enable equal-cost multi-path (ECMP) routing when multiple remote sites connect with overlapping subnets?

- A. Set route-overlap to either use-new or use-old
- B. Set net-device to ecmp
- C. Set single-source to enable

D. Set route-overlap to allow

**Answer:** A

**NEW QUESTION 40**

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

**NEW QUESTION 45**

Refer to the exhibit, which shows the packet capture output of a three-way handshake between FortiGate and FortiManager Cloud.

### Packet capture output of three-way handshake between a FortiGate and a FortiManager Cloud

```

> Frame 35: 1034 bytes on wire (8272 bits), 1034 bytes captured (8272 bits) on interface -, id 0
> Ethernet II, Src: 50:e5:d5: (50:e5:d5: ), Dst: Fortinet_ (e0:23:ff: )
> Internet Protocol Version 4, Src: 192.168.2.60, Dst: 154.52.4.164
> Transmission Control Protocol, Src Port: 16304, Dst Port: 541, Seq: 1, Ack: 1, Len: 980
▼ Transport Layer Security
  ▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 975
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 971
  > Version: TLS 1.2 [0x0303]
    Random: a14f6c4b8f9313bf
    Session ID Length: 32
    Session ID: a0de426e96e83a5
    Cipher Suites Length: 34
  > Cipher Suites (17 suites)
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 864
  ▼ Extension: server_name (len=45) name=9398.support.fortinet-ca2.fortinet.com
    Type: server_name (0)
    Length: 45
  ▼ Server Name Indication extension
    Server Name list length: 43
    Server Name Type: host_name (0)
    Server Name length: 40
    Server Name: 9398.support.fortinet-ca2.fortinet.com
  > Extension: ec_point_formats (len=4)
  > Extension: supported_groups (len=22)
  > Extension: session_ticket (len=0)
  > Extension: encrypt_then_mac (len=0)
  > Extension: extended_master_secret (len=0)
  > Extension: signature_algorithms (len=48)
  > Extension: supported_versions (len=9) TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0
  > Extension: psk_key_exchange_modes (len=2)
  
```

What two conclusions can you draw from the exhibit? (Choose two.)

- A. FortiGate will receive a certificate that supports multiple domains because FortiManager operates in a cloud computing environment.
- B. FortiGate is connecting to the same IP server and will receive an independent certificate for its connection between FortiGate and FortiManager Cloud.
- C. If the TLS handshake contains 17 cipher suites it means the TLS version must be 1.0 on this three-way handshake.
- D. The wildcard for the domain \*.fortinet-ca2.support.fortinet.com must be supported by FortiManager Cloud.

Answer: D

#### NEW QUESTION 50

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **FCSS\_EFW\_AD-7.6 Practice Exam Features:**

- \* FCSS\_EFW\_AD-7.6 Questions and Answers Updated Frequently
- \* FCSS\_EFW\_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- \* FCSS\_EFW\_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* FCSS\_EFW\_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The FCSS\\_EFW\\_AD-7.6 Practice Test Here](#)**