

# Fortinet

## Exam Questions FCSS\_EFW\_AD-7.6

FCSS - Enterprise Firewall 7.6 Administrator



**NEW QUESTION 1**

A company's users on an IPsec VPN between FortiGate A and B have experienced intermittent issues since implementing VXLAN. The administrator suspects that packets exceeding the 1500-byte default MTU are causing the problems.

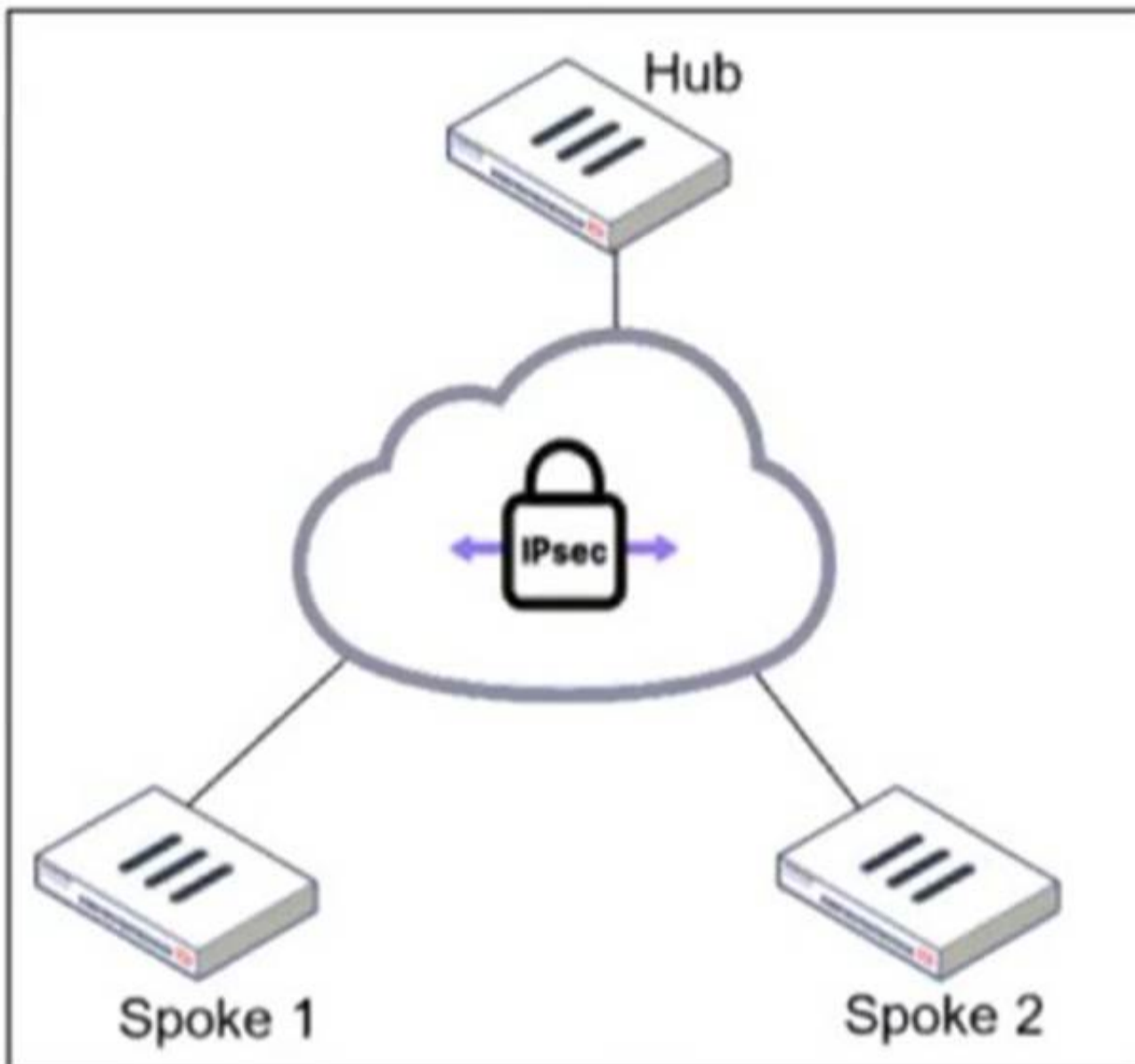
In which situation would adjusting the interface's maximum MTU value help resolve issues caused by protocols that add extra headers to IP packets?

- A. Adjust the MTU on interfaces only if FortiGate has the FortiGuard enterprise bundle, which allows MTU modification.
- B. Adjust the MTU on interfaces in all FortiGate devices that support the latest family of Fortinet SPUs: NP7, CP9 and SP5.
- C. Adjust the MTU on interfaces in controlled environments where all devices along the path allow MTU interface changes.
- D. Adjust the MTU on interfaces only in wired connections like PPPoE, optic fiber, and ethernet cable.

**Answer: C**

**NEW QUESTION 2**

Refer to the exhibit.



An administrator is deploying a hub and spokes network and using OSPF as dynamic protocol. Which configuration is mandatory for neighbor adjacency?

- A. Set bfd enable in the router configuration
- B. Set network-type point-to-multipoint in the hub interface
- C. Set rfc1583-compatible enable in the router configuration
- D. Set virtual-link enable in the hub interface

**Answer: B**

**NEW QUESTION 3**

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**

**NEW QUESTION 4**

Refer to the exhibits.

# 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 style="border: 1px solid #ccc; padding: 2px; display: inline-block;">  port1 <span style="float: right;">✕</span> </div> <div style="text-align: center; margin-top: 5px;">+</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 style="text-align: center; margin-top: 5px;"> <a href="#">Advanced Options</a> </div>
Mode	Service Provider (SP)
Default login page	<input checked="" type="radio"/> Normal <input type="radio"/> Single Sign-On
Default admin profile	super_admin_readonly
Management IP/FQDN	<input type="checkbox"/> Use WAN IP <input checked="" type="checkbox"/> Specify <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">10.1.0.100</div>
Management port	<input type="checkbox"/> Use Admin Port <input checked="" type="checkbox"/> Specify <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">443</div>

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

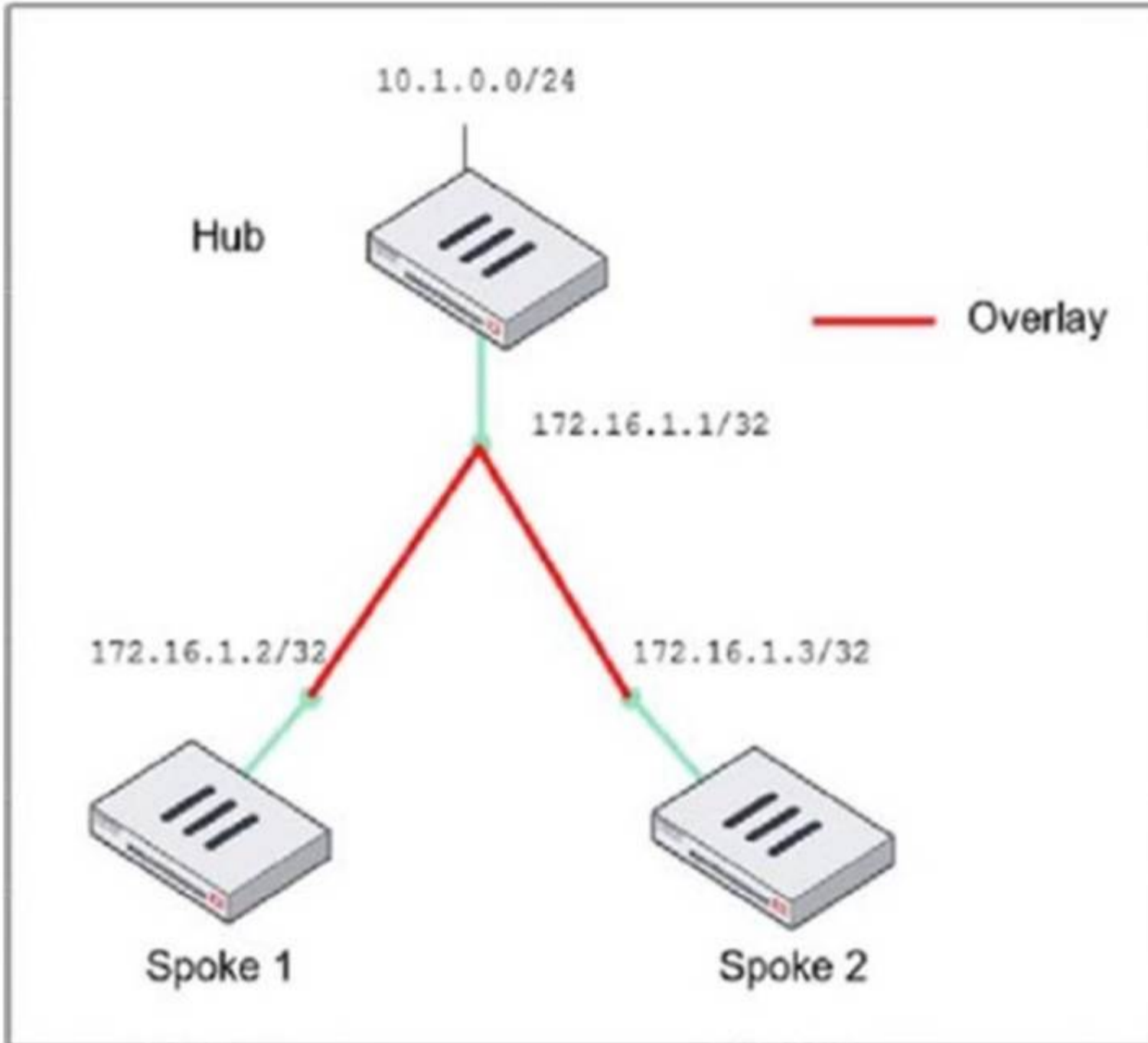
- A. The user is prompted to create an SSO administrator account for AdminSSO.
- B. The user receives an authentication failure message.
- C. The user accesses the downstream FortiGate with super\_admin\_readonly privileges.
- D. The user accesses the downstream FortiGate with super\_admin privileges.

Answer: C

### NEW QUESTION 5

Refer to the exhibit, which shows the ADVPN network topology and partial BGP configuration.

## ADVPN network topology



## Partial BGP configuration

```

Hub # config router bgp
set as 65100
set router-id 172.16.1.1
config neighbor-group
  edit "advpn"
  set remote-as 65100
  ...
end
config neighbor-range
  edit 1
  end
config network
  ..
end
  
```

Which two parameters must an administrator configure in the config neighbor range for spokes shown in the exhibit? (Choose two.)

- A. set max-neighbor-num 2
- B. set neighbor-group advpn
- C. set route-reflector-client enable
- D. set prefix 172.16.1.0 255.255.255.0

**Answer:** BD

**NEW QUESTION 6**

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 7**

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

**NEW QUESTION 8**

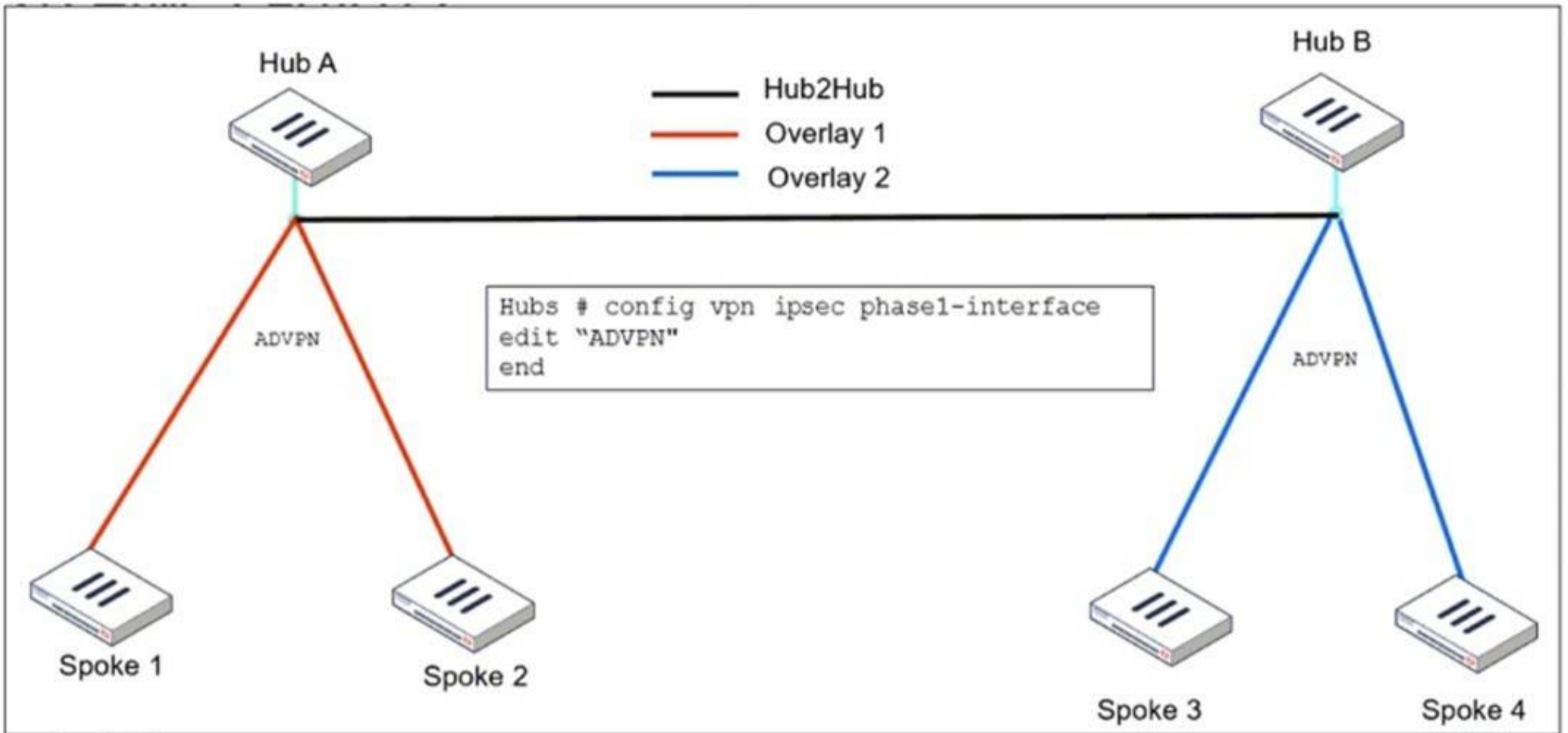
A FortiGate device with UTM profiles is reaching the resource limits, and the administrator expects the traffic in the enterprise network to increase. The administrator has received an additional FortiGate of the same model. Which two protocols should the administrator use to integrate the additional 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 9**

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 10**

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 10**

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 11**

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 14**

Which two statements about IKEv2 are true if an administrator decides to implement IKEv2 in the VPN topology? (Choose two.)

- A. It includes stronger Diffie-Hellman (DH) groups, such as Elliptic Curve (ECP) groups.
- B. It supports interoperability with devices using IKEv1.
- C. It exchanges a minimum of two messages to establish a secure tunnel.
- D. It supports the extensible authentication protocol (EAP).

**Answer: AD**

**NEW QUESTION 18**

An administrator configured the FortiGate devices in an enterprise network to join the Fortinet Security Fabric. The administrator has a list of IP addresses that must be blocked by the data center firewall. This list is updated daily. How can the administrator automate a firewall policy with the daily updated list?

- A. With FortiNAC
- B. With FortiAnalyzer
- C. With a Security Fabric automation
- D. With an external connector from Threat Feeds

**Answer:** D

**NEW QUESTION 19**

.....

## **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](#)**