

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, which shows a partial troubleshooting command output.

```
FortiGate # diagnose vpn tunnel list name Hub2Spoke1
list ipsec tunnel by names in vd 0
...
npu_flag=20 npu_rgwy=10.10.2.2 npu_lgwy=10.10.1.1 npu_selid=1
```

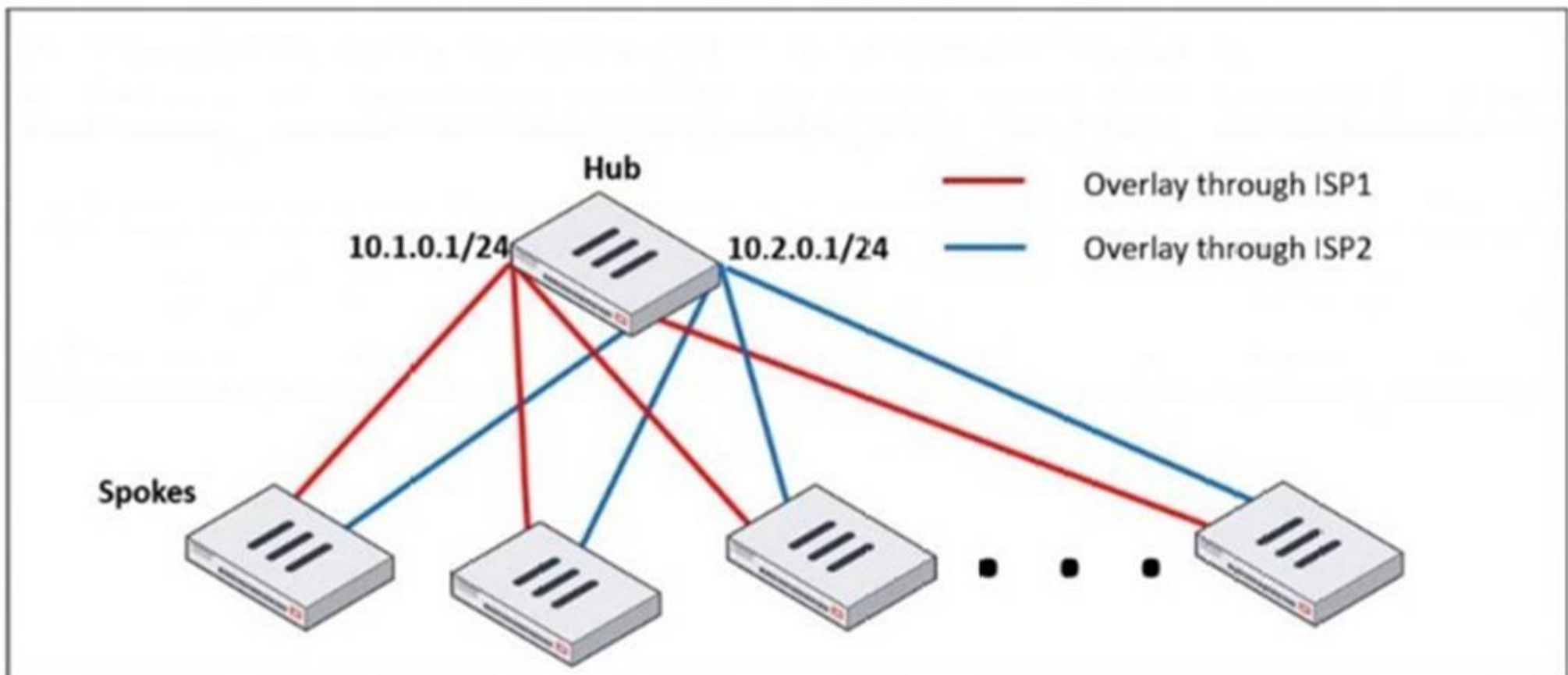
An administrator is extensively using IPsec on FortiGate. Many tunnels show information similar to the output shown in the exhibit. What can the administrator conclude?

- 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: B

NEW QUESTION 3

Refer to the exhibit, which shows a hub and spokes deployment.



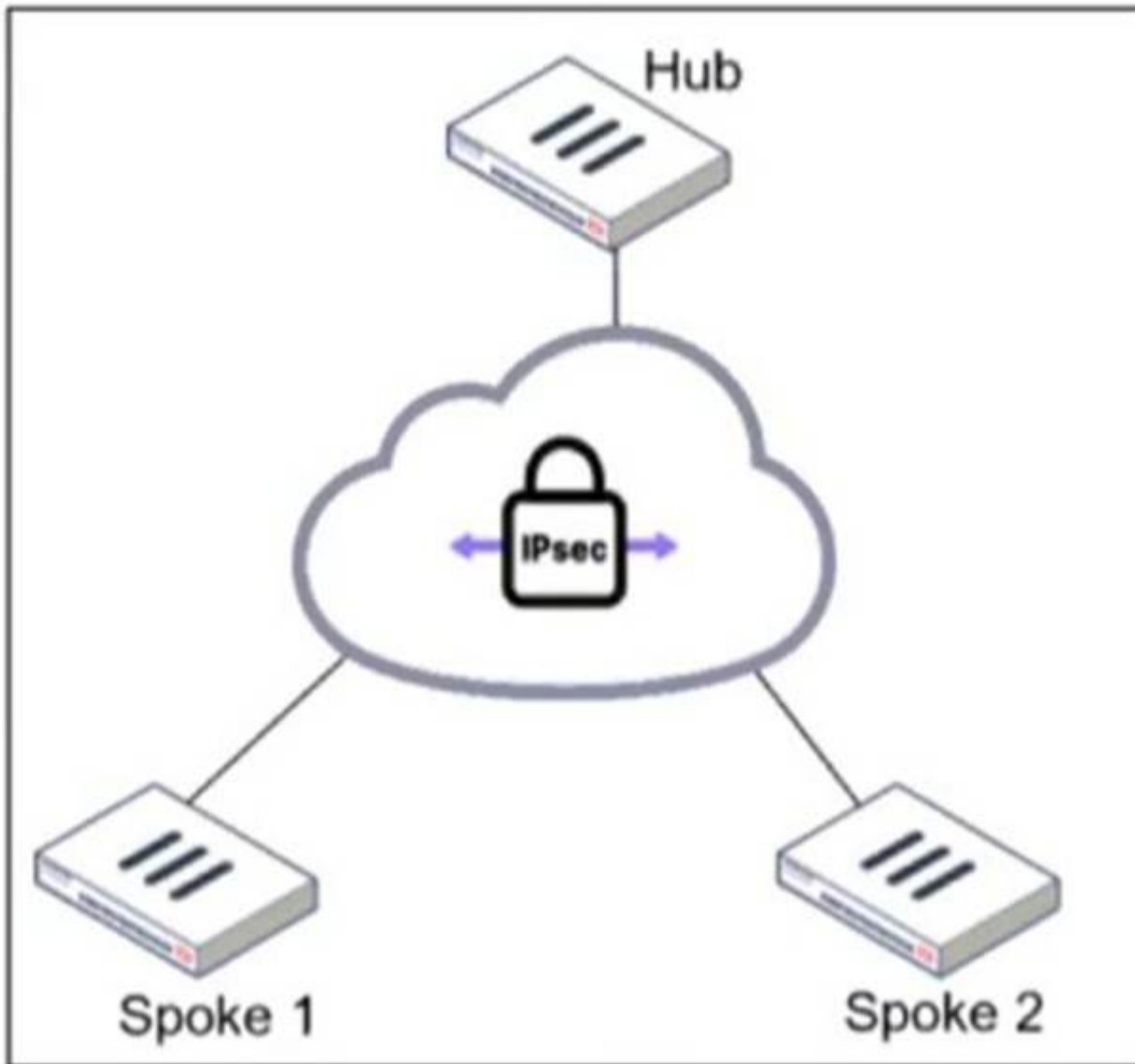
An administrator is deploying several spokes, including the BGP configuration for the spokes to connect to the hub. Which two commands allow the administrator to minimize the configuration? (Choose two.)

- A. neighbor-group
- B. route-reflector-client
- C. neighbor-range
- D. ibgp-enforce-multihop

Answer: AC

NEW QUESTION 4

Refer to the exhibit.



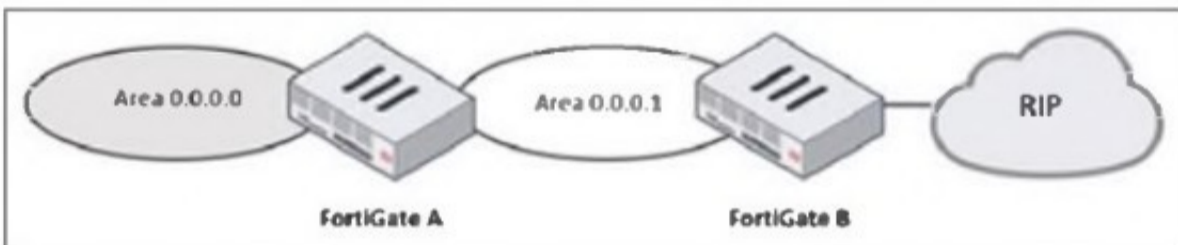
An administrator is deploying a hub and spokes network and using OSPF as dynamic protocol. Which configuration is mandatory for neighbor adjacency?

- 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 5

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?

- 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 0.0.0.1 type to stub on FortiGate A and B.

Answer: A

NEW QUESTION 6

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 ✕ </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;"> Advanced Options </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?

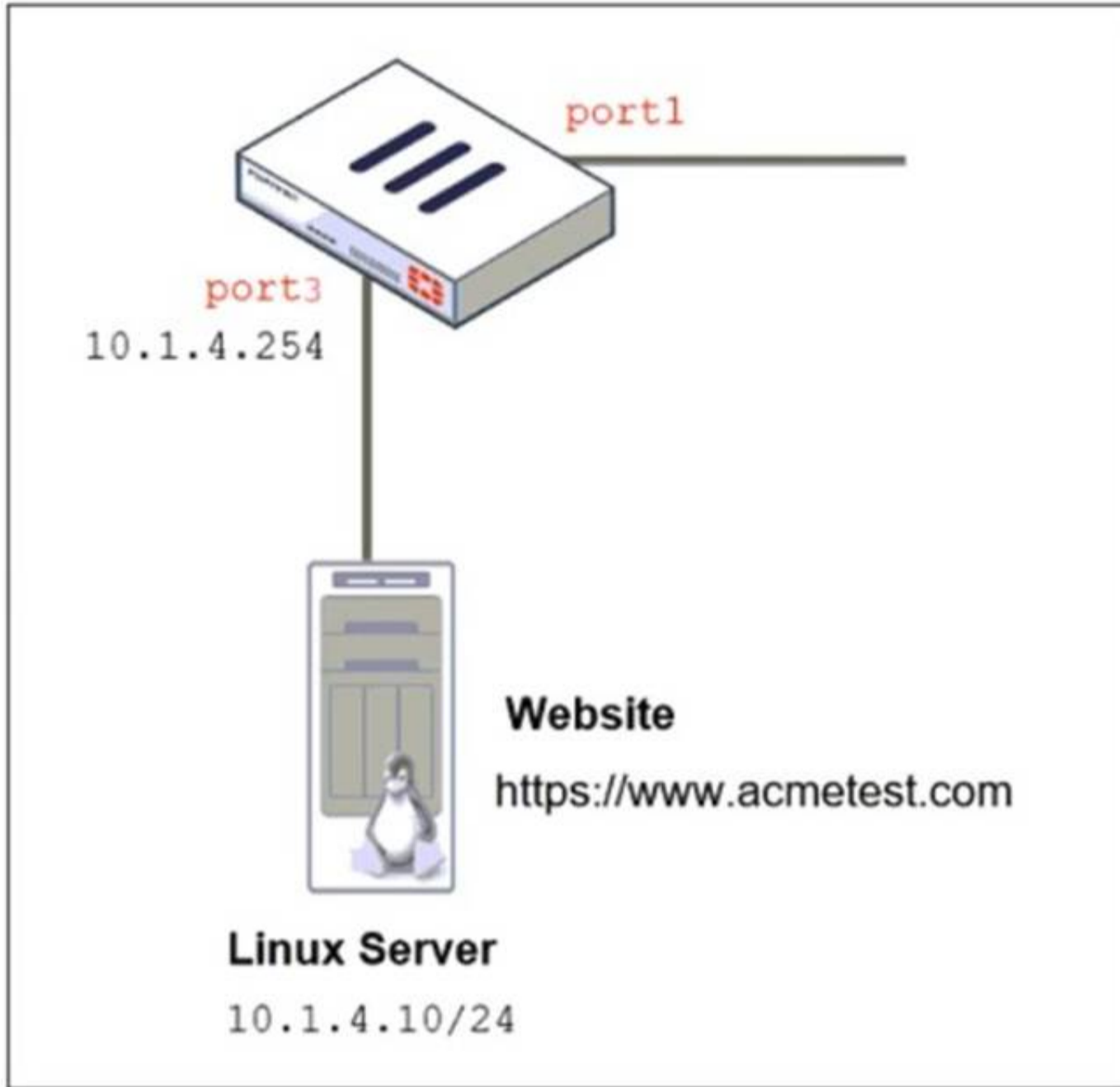
- A. The user is prompted to create an SSO administrator account for AdminSSO.
- B. The user receives an authentication failure message.
- C. The user accesses the downstream FortiGate with super_admin_readonly privileges.
- D. The user accesses the downstream FortiGate with super_admin privileges.

Answer: C

NEW QUESTION 7

Refer to the exhibits. The exhibits show a network topology, a firewall policy, and an SSL/SSH inspection profile configuration.

Network Topology



Firewall policy on FortiGate

```
DCFW # sh firewall policy 3
config firewall policy
edit 3
set name "To Linux Servers"
set uuid bf77d59e-5513-51ef-147d-e35066c267e9
set srcintf "port1"
set dstintf "port3"
set action accept
set srcaddr "all"
set dstaddr "10.1.4."
set schedule "always"
set service "ALL"
set utm-status enable
set inspection-mode proxy
set ssl-ssh-profile "deep-inspection"
set ips-sensor "IPS Monitor"
set logtraffic all
next
end
```

SSL/SSH inspection profile

Edit SSL/SSH Inspection Profile

Name

Comments 34/255

SSL Inspection Options

Enable SSL inspection of Multiple Client Connections Connecting to Multiple Servers

Inspection method Full SSL Inspection

CA certificate ⚠ Download

Blocked certificates i Block View Blocked Certificates

Untrusted SSL certificates Allow Block Ignore View Trusted CAs List

Server certificate SNI check i Enable Strict Disable

Enforce SSL cipher compliance

Enforce SSL negotiation compliance

RPC over HTTPS

MAPI over HTTPS

Protocol Port Mapping

Inspect all ports

HTTPS	<input type="checkbox"/>	443
SMTS	<input checked="" type="checkbox"/>	465
POP3S	<input checked="" type="checkbox"/>	995
IMAPS	<input checked="" type="checkbox"/>	993
FTPS	<input checked="" type="checkbox"/>	990
DNS over TLS	<input type="checkbox"/>	853

Why is FortiGate unable to detect HTTPS attacks on firewall policy ID 3 targeting the Linux server?

- A. The administrator must set the policy to inspection mode to analyze the HTTPS packets as expected.
- B. The administrator must enable HTTPS in the protocol port mapping of the deep- inspection SSL/SSH inspection profile.
- C. The administrator must enable SSL inspection of the SSL server and upload the certificate of the Linux server website to the SSL/SSH inspection profile.
- D. The administrator must enable cipher suites in the SSL/SSH inspection profile to decrypt the message.

Answer: C

NEW QUESTION 8

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 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

An administrator is extensively using VXLAN on FortiGate. Which specialized acceleration hardware does FortiGate need to improve its performance?

- A. NP7
- B. SP5
- C. 9
- D. NTurbo

Answer: A

NEW QUESTION 10

A user reports that their computer was infected with malware after accessing a secured HTTPS website. However, when the administrator checks the FortiGate logs, they do not see that the website was detected as insecure despite having an SSL certificate and correct profiles applied on the policy. How can an administrator ensure that FortiGate can analyze encrypted HTTPS traffic on a website?

- A. The administrator must enable reputable websites to allow only SSL/TLS websites rated by FortiGuard web filter.
- B. The administrator must enable URL extraction from SNI on the SSL certificate inspection to ensure the TLS three-way handshake is correctly analyzed by FortiGate.
- C. The administrator must enable DNS over TLS to protect against fake Server Name Indication (SNI) that cannot be analyzed in common DNS requests on HTTPS websites.
- D. The administrator must enable full SSL inspection in the SSL/SSH Inspection Profile to decrypt packets and ensure they are analyzed as expected.

Answer: D

NEW QUESTION 13

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	DCFW	admin	Installed	

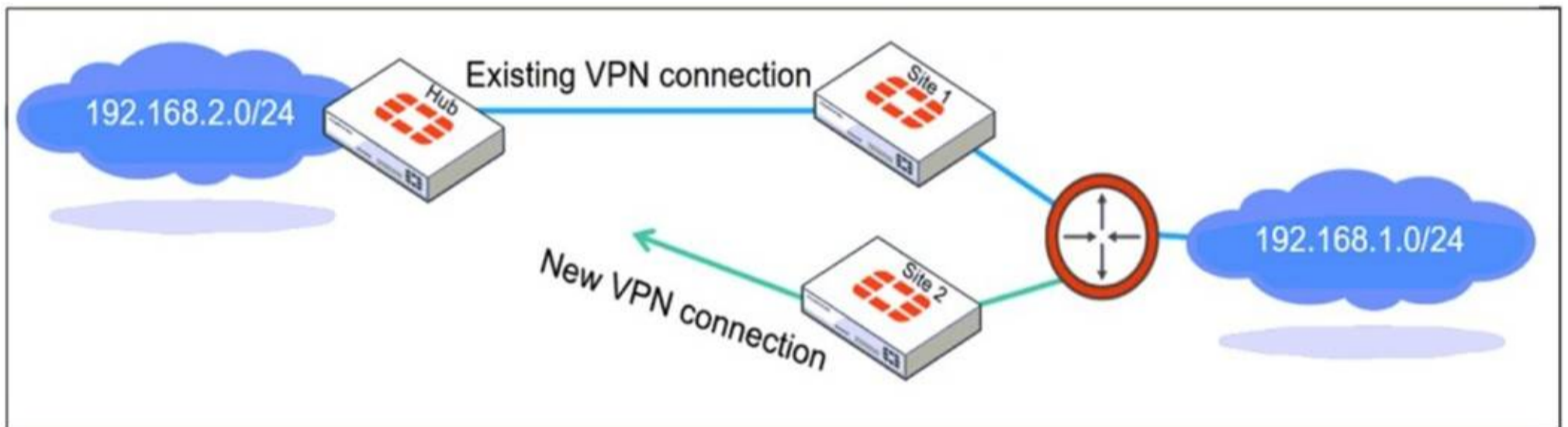
The IT team is trying to identify the administrator responsible for the most recent update in the FortiGate device database. Which conclusion can you draw about this scenario?

- 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 18

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 20

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 23

Refer to the exhibit.

Routing table on FortiGate_A

```
FortiGate_A # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
V - BGP VPNv4
* - candidate default

Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 10.1.0.254, port1, [1/0]
C 10.1.0.0/24 is directly connected, port1
C 10.1.4.0/24 is directly connected, port3
B 100.64.1.0/24 [200/0] via 10.1.0.254 (recursive is directly connected, port1), 00:39:45, [1/0]
B 172.16.1.252/30 [200/0] via 10.1.0.1 (recursive is directly connected, port1), 00:42:48, [1/0]
C 172.16.100.0/24 is directly connected, port8
```

Routing table on FortiGate_B

```
FortiGate_B # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
V - BGP VPNv4
* - candidate default

Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 10.1.0.254, port1, [1/0]
S 4.2.2.2/32 [10/0] via 10.1.5.254, port4, [1/0]
C 10.1.0.0/24 is directly connected, port1
B 10.1.4.0/24 [200/0] via 10.1.0.100 (recursive is directly connected, port1), 00:41:02, [1/0]
C 10.1.5.0/24 is directly connected, port4
B 100.64.1.0/24 [200/0] via 10.1.0.254 (recursive is directly connected, port1), 00:38:14, [1/0]
C 172.16.1.248/30 is directly connected, C0
C 172.16.1.252/30 is directly connected, A0
C 172.16.100.0/24 is directly connected, port8
```

The routing tables of FortiGate_A and FortiGate_B are shown. FortiGate_A and FortiGate_B are in the same autonomous system. The administrator wants to dynamically add only route 172.16.1.248/30 on FortiGate_A. What must the administrator configure?

- A. The prefix 172.16.1.248/30 in the BGP Networks section on FortiGate_B
- B. A BGP route map out for 172.16.1.248/30 on FortiGate_B
- C. Enable Redistribute Connected in the BGP section on FortiGate_B.
- D. A BGP route map in for 172.16.1.248/30 on FortiGate_A

Answer: B

NEW QUESTION 25

.....

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](#)