Question #1 *Topic 1*

You 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 reduces system load while also enabling security features, such as web filtering and application control for encrypted HTTPS traffic?

A. Enable SSL certificate inspection mode to perform basic checks without decrypting traffic.

B. Disable SSL inspection to preserve resources.

C. Use deep SSL inspection to inspect encrypted HTTPS traffic.

D. Configure SSL inspection to handle HTTPS traffic efficiently.

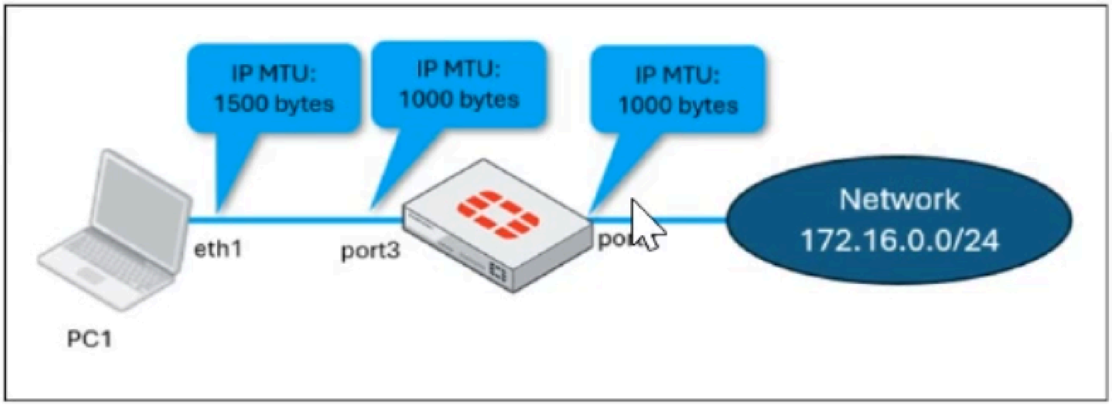
Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

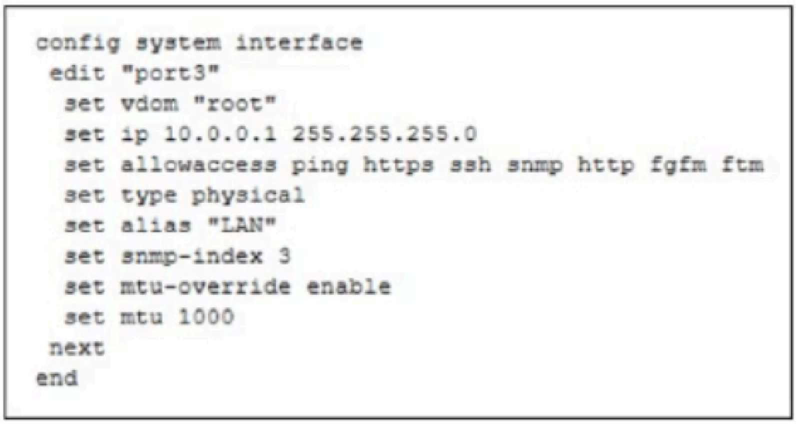
Question #2 *Topic 1*

Refer to the exhibits.

Network topology

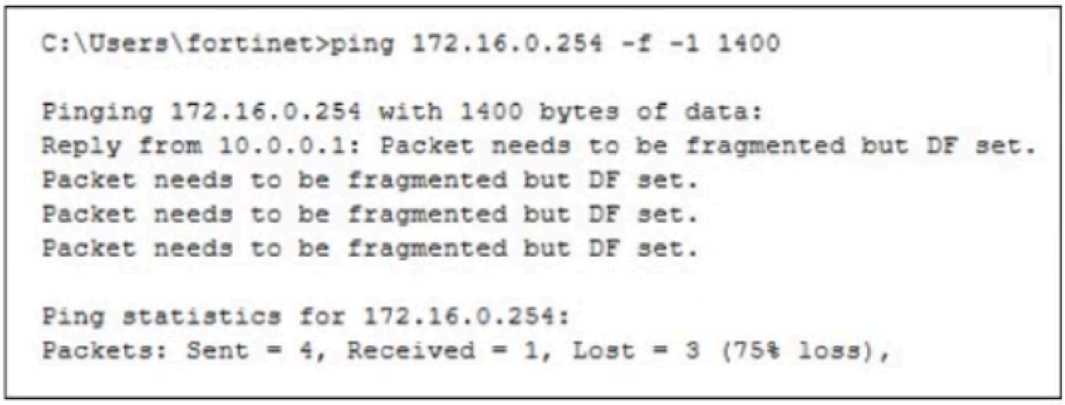


port 3 configuration on FortiGate



```
config system interface
 edit "port3"
  set vdom "root"
  set ip 10.0.0.1 255.255.255.0
  set allowaccess ping https ssh snmp http fgfm ftm
  set type physical
  set alias "LAN"
  set snmp-index 3
  set mtu-override enable
  set mtu 1000
 next
end
```

ping output



```
C:\Users\fortinet>ping 172.16.0.254 -f -l 1400

Pinging 172.16.0.254 with 1400 bytes of data:
Reply from 10.0.0.1: Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 172.16.0.254:
Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
```

The configuration of Windows PC, PC 1, with a default MTU of 1500 bytes, FortiGate interfaces with an MTU of 1000 bytes, and the results of PC 1 pinging over server 172.16.0.251 are shown.
Why is the PC1 user unable to ping server 172.16.0.254 and seeing the message: Packet needs to be fragmented but DF set?

A. The user must adjust the TCP maximum segment size (MSS) to 1000 for the ping to succeed

B. The ip.flags.mf option must be enabled on FortiGate. The user must adjust the ping MTU to 1000 to succeed.

C. The user must account for the size of the Ethernet header when configuring the MTU value.

D. FortiGate honors the do not fragment bit and the packets are dropped. The user must adjust the ping MTU to 972 to succeed.

Suggested Answer: *D*

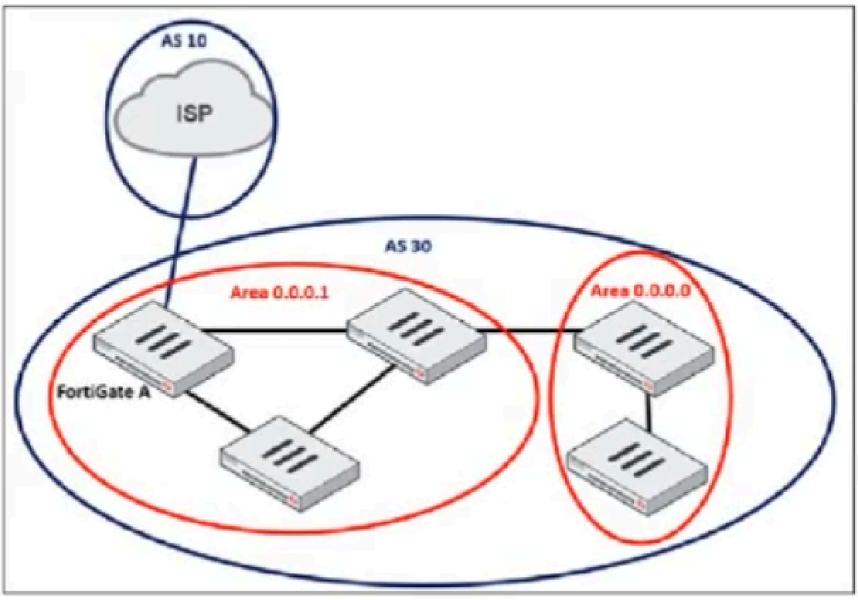
Currently there are no comments in this discussion, be the first to comment!

Question #3

Topic 1

Refer to the exhibit.

An enterprise network connected to an ISP is shown.



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

Which two commands must you use to establish the connection? (Choose two.)

A. ibgp-enforce-multihop

B. ebgp-enforce-multihop

C. recursive-next-hop

D. update-source

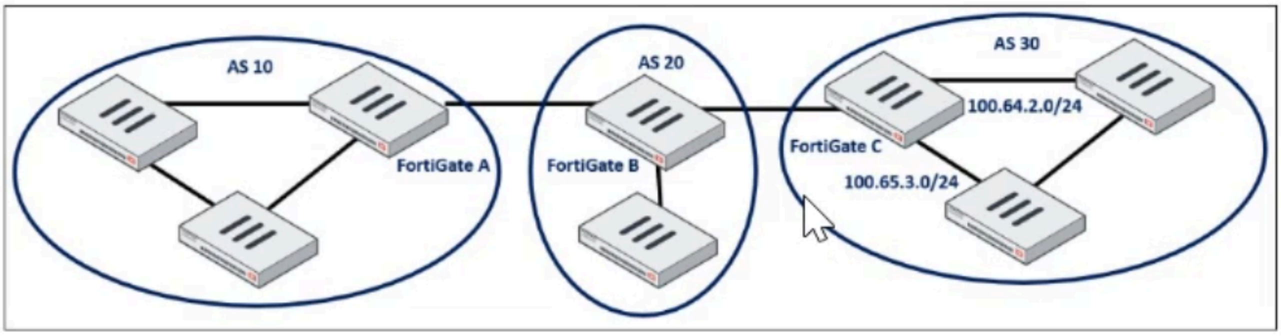
Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

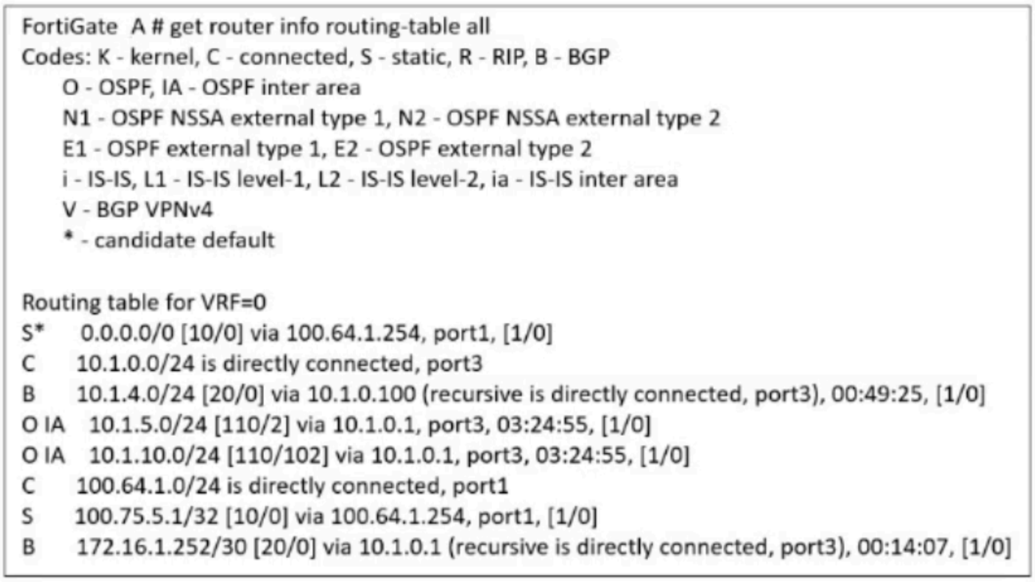
Question #4 Topic 1

Refer to the exhibit.

Network topology



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 100.64.1.254, port1, [1/0]
C      10.1.0.0/24 is directly connected, port3
B      10.1.4.0/24 [20/0] via 10.1.0.100 (recursive is directly connected, port3), 00:49:25, [1/0]
O IA   10.1.5.0/24 [110/2] via 10.1.0.1, port3, 03:24:55, [1/0]
O IA   10.1.10.0/24 [110/102] via 10.1.0.1, port3, 03:24:55, [1/0]
C      100.64.1.0/24 is directly connected, port1
S      100.75.5.1/32 [10/0] via 100.64.1.254, port1, [1/0]
B      172.16.1.252/30 [20/0] via 10.1.0.1 (recursive is directly connected, port3), 00:14:07, [1/0]
```

A network topology and a FortiGate routing table is shown.

What must you configure in the BGP section to add only the subnet 100.64.2.0/24 in the routing table of FortiGate_A?

A. Configure route-map-in on FortiGate_A.

B. Configure connected routes redistribution on FortiGate_C.

C. Configure BGP route redistribution on FortiGate_B.

D. Configure the 100.64.2.0/24 network on FortiGate_C.

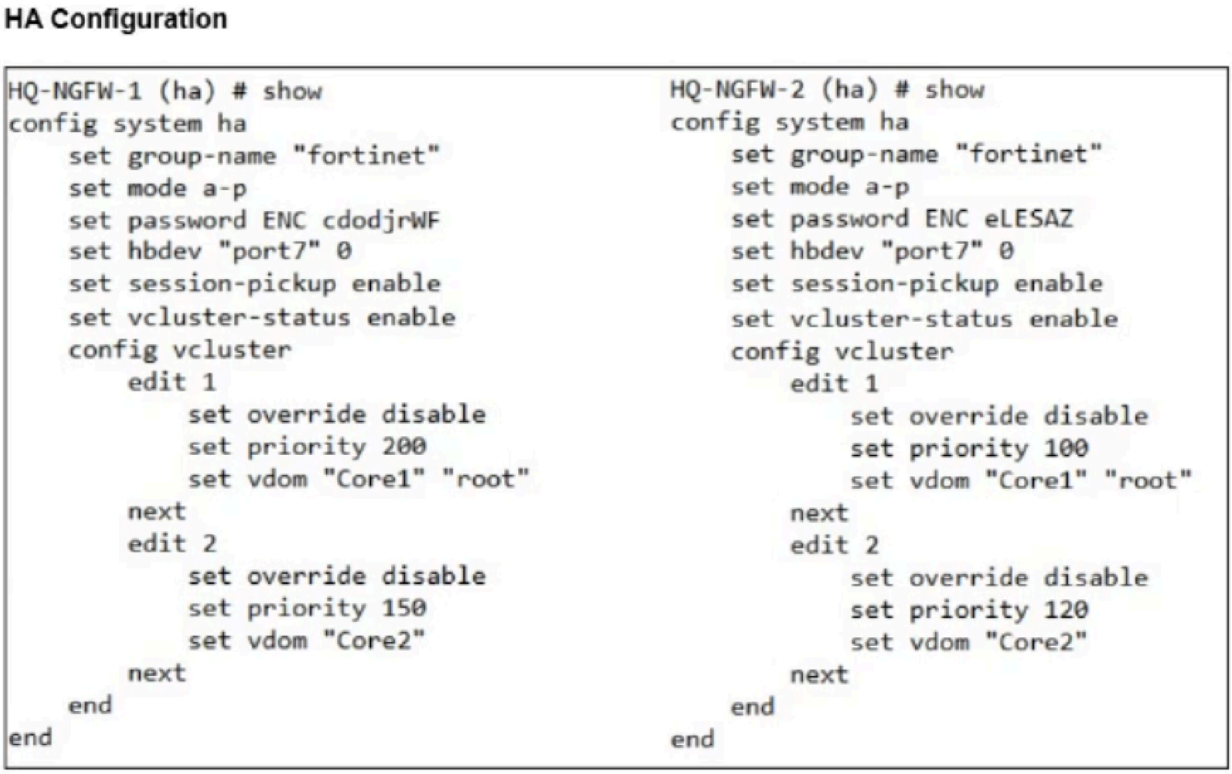
Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #5

Topic 1

Refer to the exhibit.



HA Configuration

```
HQ-NGFW-1 (ha) # show
config system ha
    set group-name "fortinet"
    set mode a-p
    set password ENC cdodjrWF
    set hbdev "port7" 0
    set session-pickup enable
    set vcluster-status enable
    config vcluster
        edit 1
            set override disable
            set priority 200
            set vdom "Core1" "root"
        next
        edit 2
            set override disable
            set priority 150
            set vdom "Core2"
        next
    end
end
```

```
HQ-NGFW-2 (ha) # show
config system ha
    set group-name "fortinet"
    set mode a-p
    set password ENC eLESAZ
    set hbdev "port7" 0
    set session-pickup enable
    set vcluster-status enable
    config vcluster
        edit 1
            set override disable
            set priority 100
            set vdom "Core1" "root"
        next
        edit 2
            set override disable
            set priority 120
            set vdom "Core2"
        next
    end
end
```

An HA configuration of an active-active (A-A) cluster with the same HA uptime shown.

You want HQ-NGFW-2 to handle the Core2 VDOM traffic.

Which modification must you make to achieve this outcome?

A. Enable override in virtual duster 2 for HQ-NGFW-2.

B. Change the priority from 120 to 200 for HQ-NGFW-2.

C. Change the priority from 100 to 160 for HQ-NGFW-2.

D. Reboot HQ-NGFW-2.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

You receive a FortiAnalyzer alert warning that a 1 TB disk filled up in a day. Upon investigation, you find thousands of unusual DNS log requests, such as JHCMQK.website.com, with no answers. You later discover that DNS exfiltration is occurring through both UDP and TLS.
How can you prevent this data theft technique?

A. Use a file filter profile to protect against DNS exfiltration.

B. Use an intrusion prevention system (IPS) profile and DNS exfiltration-related signatures.

C. Enable DNS filter to protect against DNS exfiltration.

D. Enable data loss prevention (DLP) to prevent DNS exfiltration.

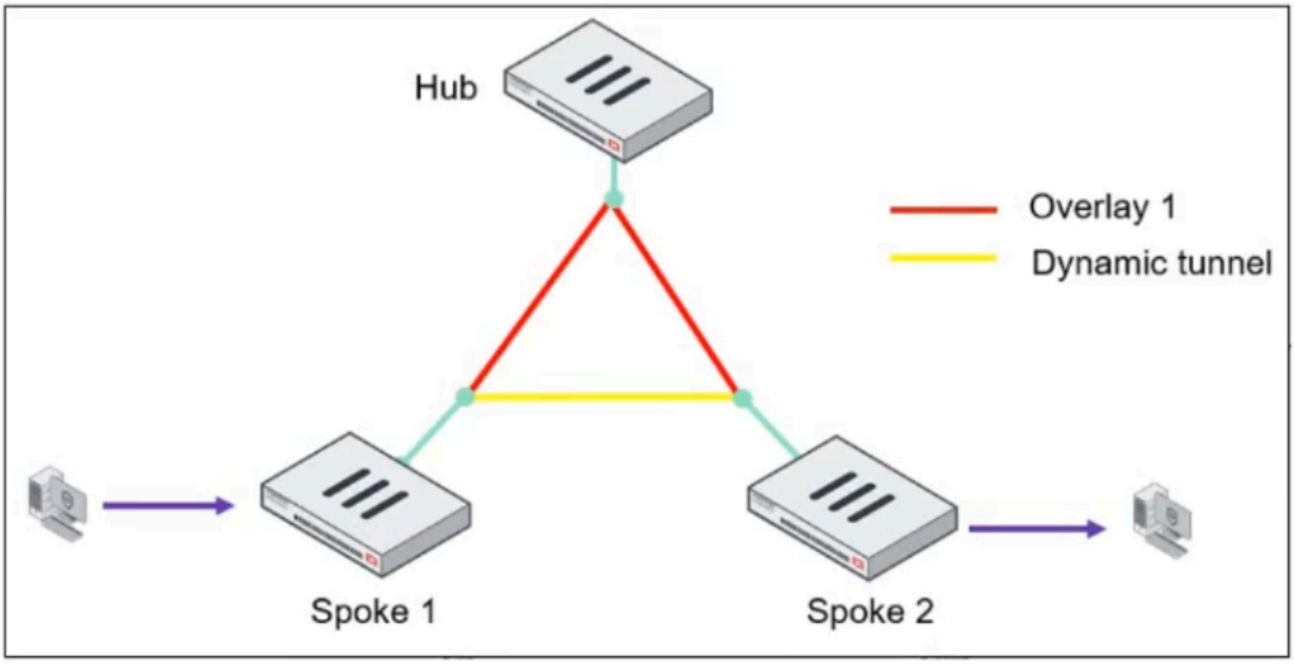
Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

Refer to the exhibit.

Network topology



Based on the exhibit, what is the first message that Spoke 1 replies to the hub instructing it to bring up the dynamic tunnel if a client generates traffic destined to Spoke 2?

A. Shortcut query

B. Shortcut forward

C. Shortcut offer

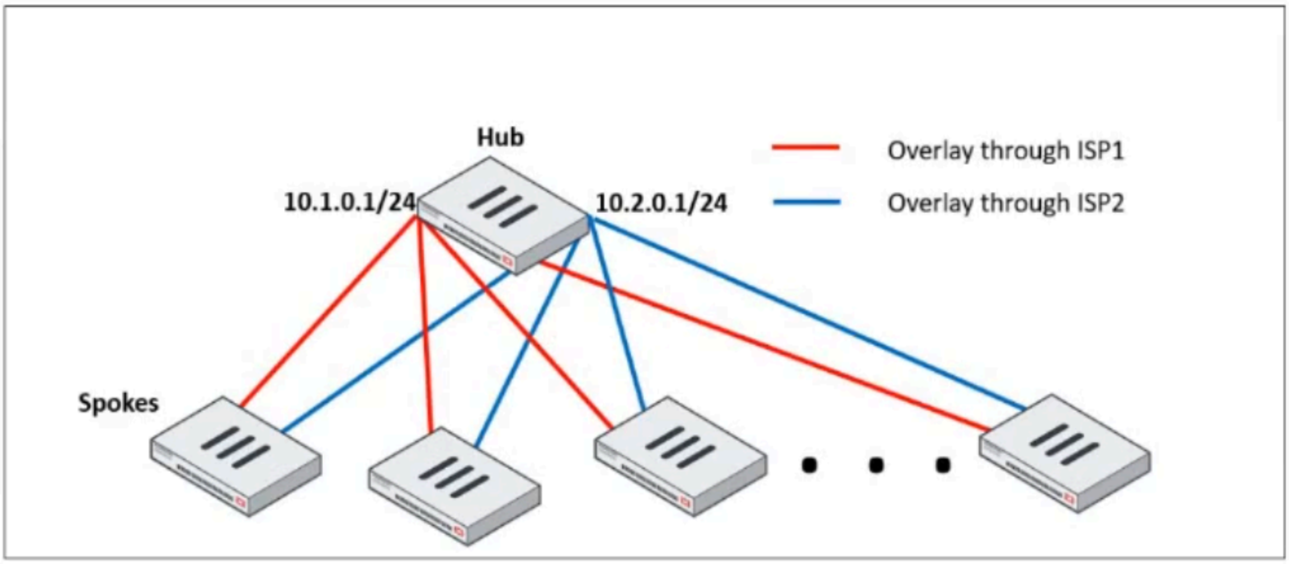
D. Shortcut reply

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibit.

Network topology



A network diagram with a hub and spokes deployment is shown.

You must deploy several spokes, including the BGP configuration for the spokes that connect to the hub.

Which two commands would you use to minimize the amount of configuration needed on the hub? (Choose two.)

A. ebgp-multipath

B. route-overlap

C. neighbor-range

D. neighbor-group

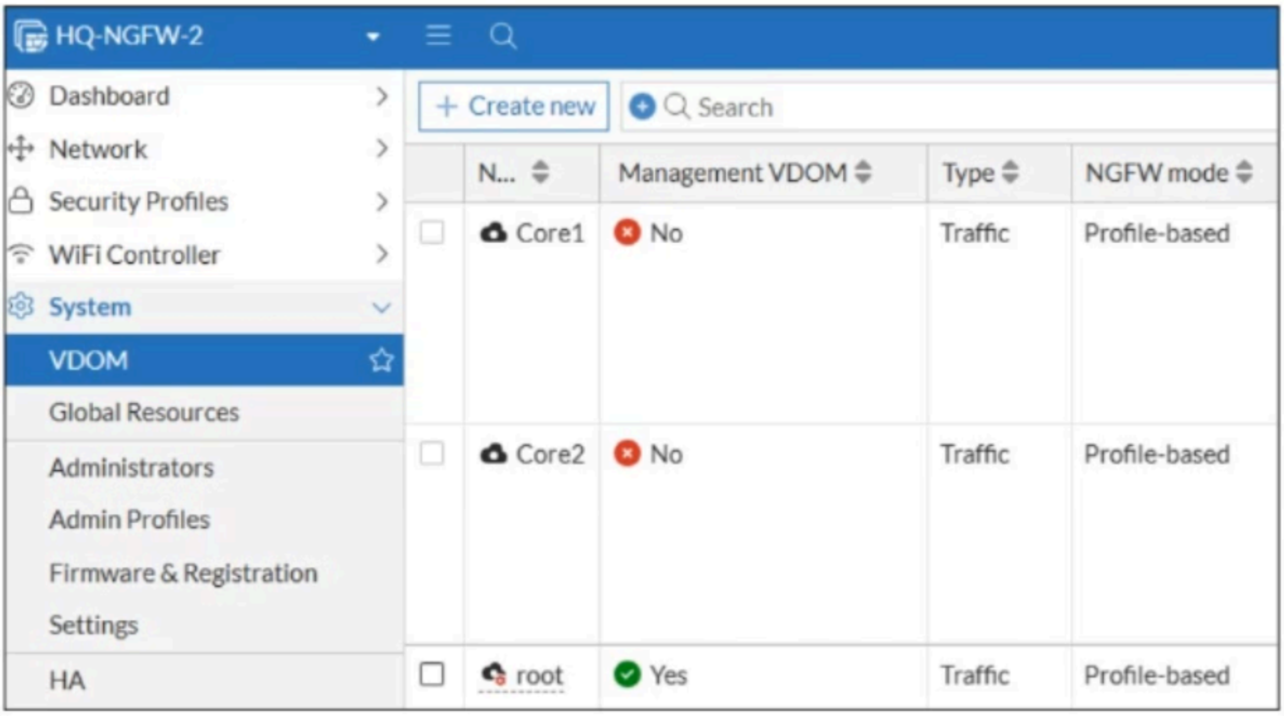
Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Refer to the exhibit.

VDOM sessions



	N...	Management VDOM	Type	NGFW mode
□	Core1	☒ No	Traffic	Profile-based
□	Core2	☒ No	Traffic	Profile-based
□	root	✓ Yes	Traffic	Profile-based

The VDOM configuration on a FortiGate device is shown.

You discover that web filtering stopped working in Corel and Core2 after a maintenance window.

What are two reasons why web filtering stopped working? (Choose two.)

A. The root VDOM does not use a VDOM link to connect with the Core1 and Core2 VDOMs.

B. The root VDOM does not have access to any valid, public Fortinet Distribution Network (FDN).

C. The root VDOM does not have access to FortiManager in a dosed network.

D. The Core1 and Core2 VDOMs must also be enabled as management VDOMs to receive FortiGuard updates.

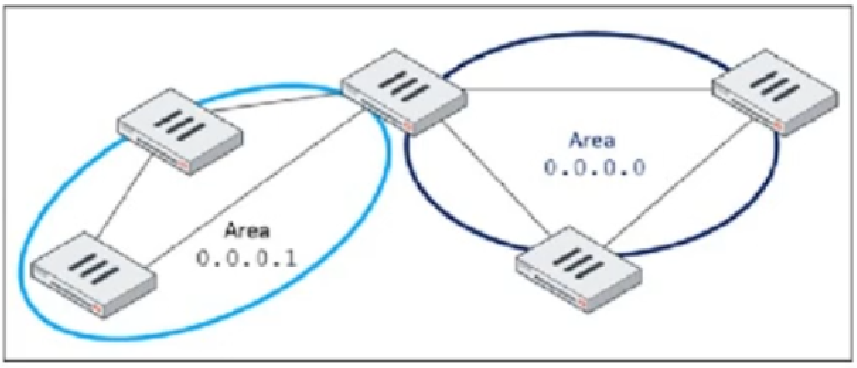
Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Refer to the exhibit.

An OSPF network is shown.



Which configuration must you apply to optimize the OSPF database?

A. Set the area 0.0.0.1 to the type Stub in the area border FortiGate.

B. Set a route map in the autonomous system boundary FortiGate.

C. Set the area 0.0.0.l to the type NSSA in the area border FortiGate.

D. Set a prefix list in the autonomous system boundary FortiGate.

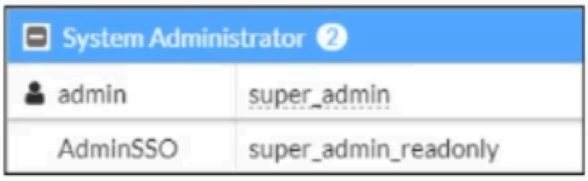
Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

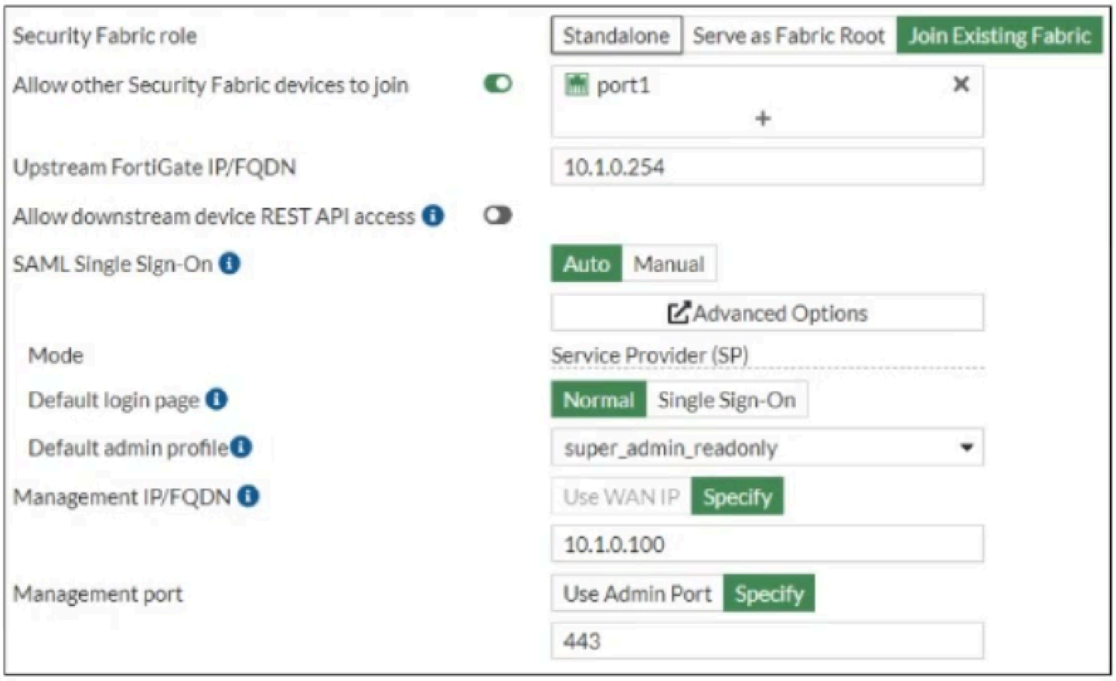
Refer to the exhibits.

Root FortiGate - System Administrator configuration



System Administrator 2	
admin	super_admin
AdminSSO	super_admin_readonly

Downstream FortiGate - Security Fabric settings



Security Fabric role: Standalone | Serve as Fabric Root | Join Existing Fabric

Allow other Security Fabric devices to join ●: port1 ✕ +

Upstream FortiGate IP/FQDN: 10.1.0.254

Allow downstream device REST API access ○

SAML Single Sign-On: Auto | Manual

Advanced Options

Mode: Service Provider (SP)

Default login page: Normal | Single Sign-On

Default admin profile: super_admin_readonly

Management IP/FQDN: Use WAN IP | Specify

10.1.0.100

Management port: Use Admin Port | Specify

443

The system administrator settings configured on a root FortiGate and the Security Fabric settings configured on a downstream FortiGate are shown.

When prompted to sign in with Security Fabric to the downstream FortiGate. a user enters the single sign-on (SSO) provider credentials.

What happens next for the user?

A. The user is redirected to the root FortiGate.

B. The user accesses the downstream FortiGate with super_admin_readonly privileges.

C. The user accesses the root FortiGate with AdminSSO privileges.

D. The user receives an authentication failure message.

Suggested Answer: *B*

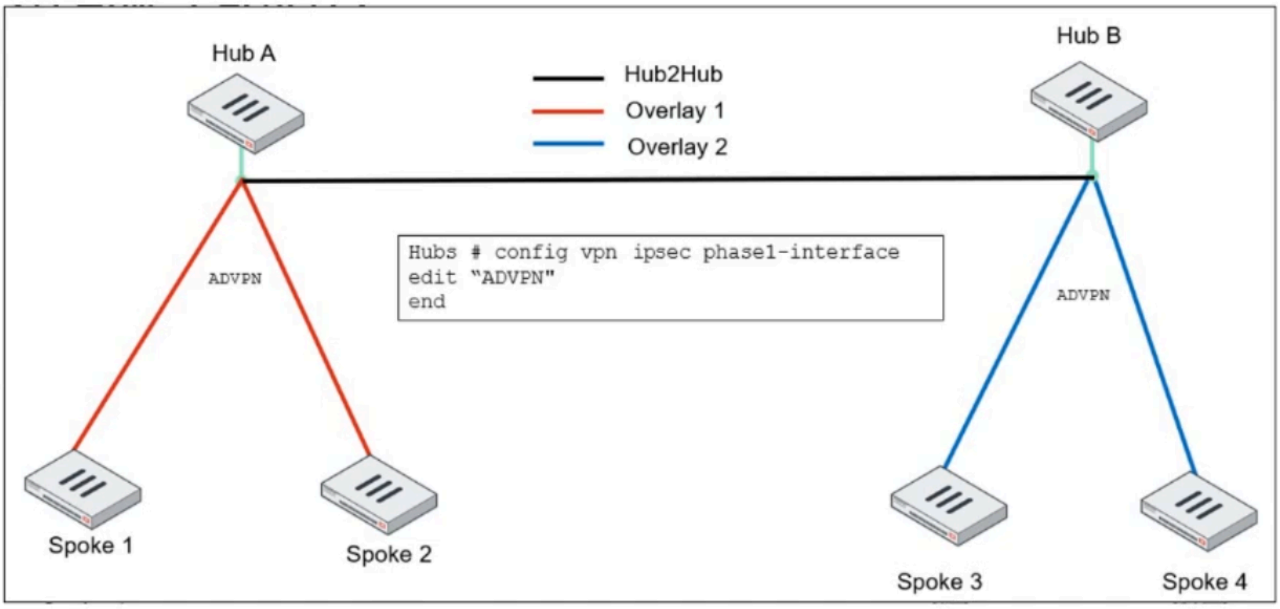
Currently there are no comments in this discussion, be the first to comment!

Question #12

Topic 1

Refer to the exhibit.

Network topology



```
Hubs # config vpn ipsec phase1-interface
edit "ADVPN"
end
```

The ADVPN IPsec interface represents the VPN IPsec phase 1 from Hub A to Spoke 1 and Spoke 2, and from Hub B to Spoke 3 and Spoke 4.

You must configure an ADVPN using IBGP and EBGP to connect Overlay 1 with Overlay 2.

Which parameters must you configure in the phase 1 VPN IPsec configuration of the ADVPN tunnels?

A. set auto-discovery-forwarder enable and set remote-as x

B. set auto-discovery-crossover enable and set enforce-multihop enable

C. set auto-discovery-sender enable and set network-id x

D. set auto-discovery-receiver enable and set remote-ip x

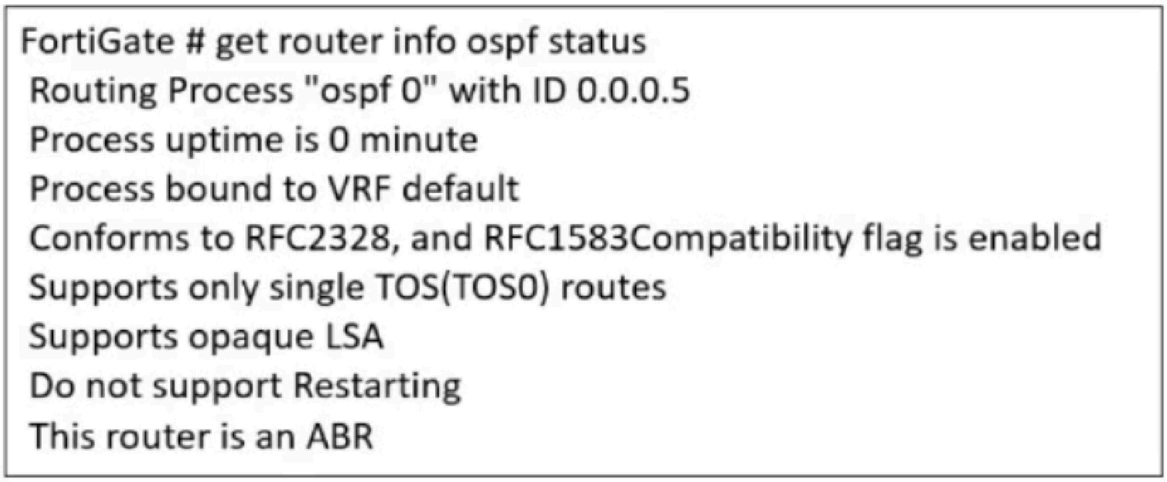
Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Refer to the exhibit.

The partial output of an OSPF command is shown.



```
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
```

While checking the OSPF status of FortiGate. you receive the output shown in the exhibit.

Based on the output, which two statements about FortiGate are correct? (Choose two.)

A. FortiGate injects external routing information.

B. FortiGate is a backup designated router.

C. FortiGate is connected to multiple areas.

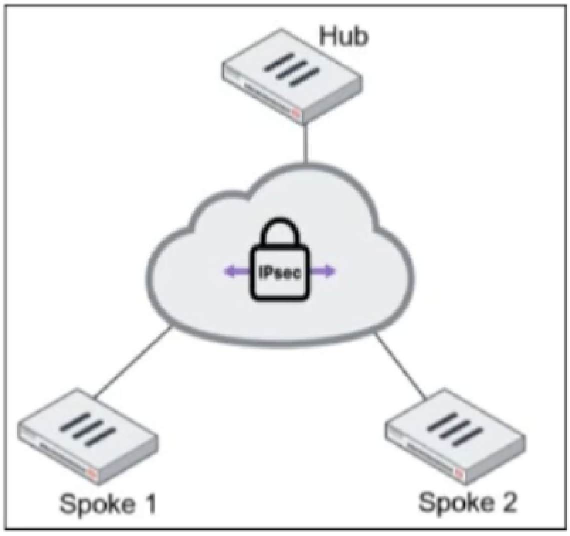
D. FortiGate has OSPF ECMP enabled.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Refer to the exhibit.



You are deploying a hub and spokes network and using OSPF as a dynamic protocol.
Which configuration is recommended for neighbor adjacency through the hub?

A. Set virtual-link enable in the OSPF configuration

B. Set rfc1583-compatible enable in the router configuration

C. Set network-type point-to-multipoint in the hub interface

D. Set route-reflector-client enable in the router configuration

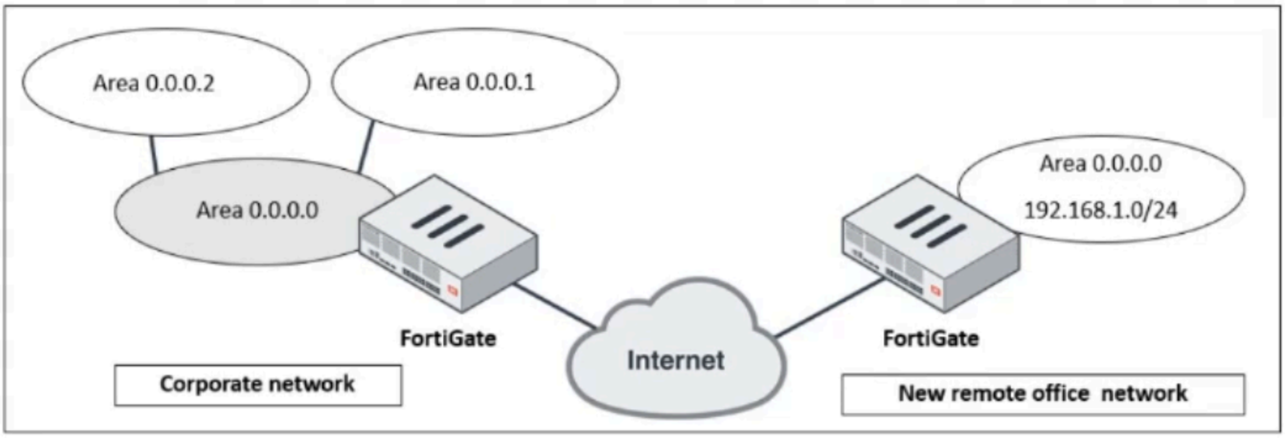
Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Refer to the exhibit.

Network topology



A network diagram showing the corporate network and a new remote office network is shown.
You must integrate the new remote office network with the corporate enterprise network.
What must you do to allow routing between the two networks?

A. Implement BGP to inject the new remote office network into the corporate FortiGate device.

B. Add the network 192.168.1.0/24 in the OSPF section on the corporate FortiGate device.

C. Implement OSPF over IPsec on both FortiGate devices.

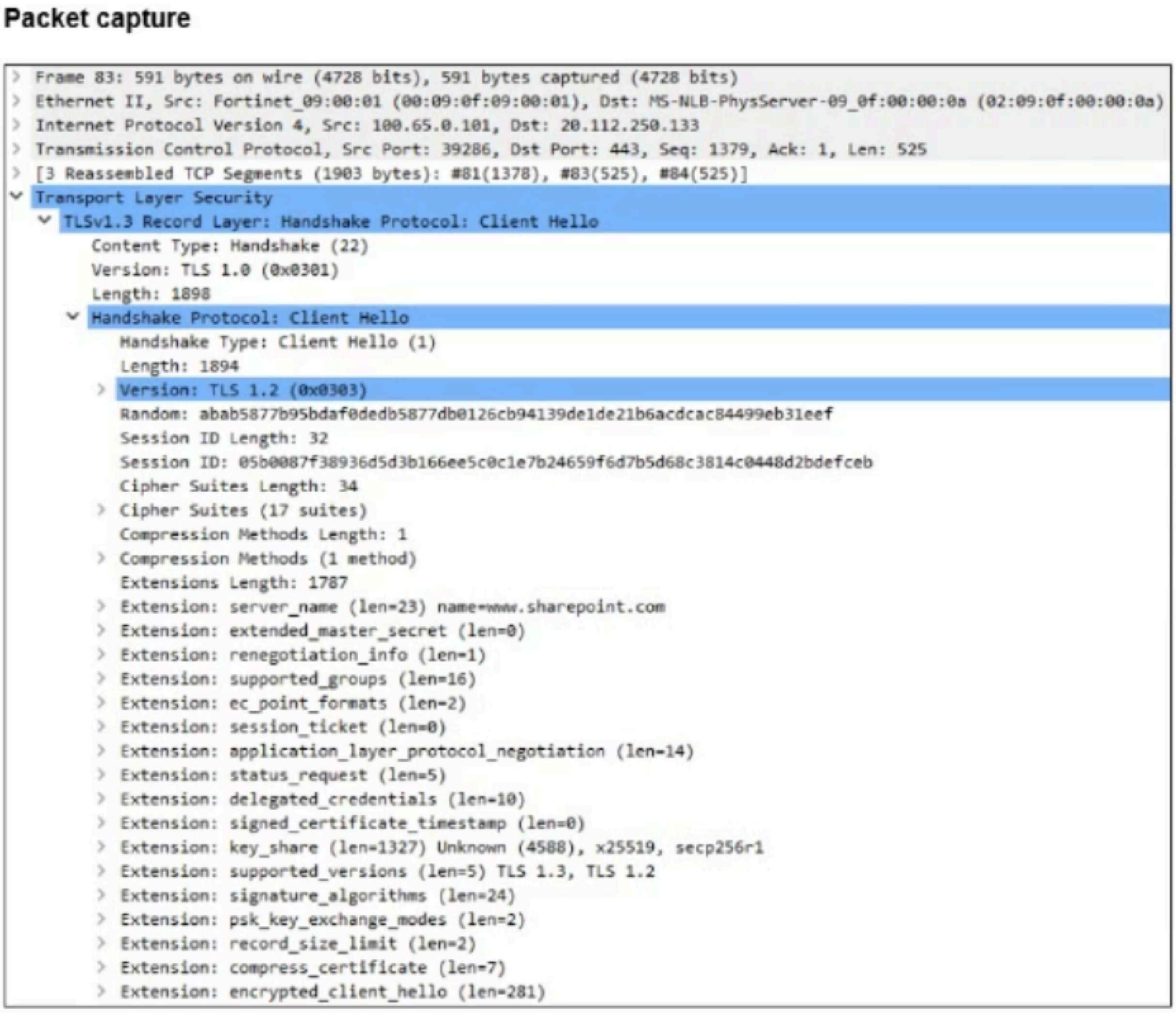
D. Configure virtual links on both FortiGate devices.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #16 Topic 1

Refer to the exhibit.



Packet capture

```
> Frame 83: 591 bytes on wire (4728 bits), 591 bytes captured (4728 bits)
> Ethernet II, Src: Fortinet_09:00:01 (00:09:0f:09:00:01), Dst: MS-NLB-PhysServer-09_0f:00:00:0a (02:09:0f:00:00:0a)
> Internet Protocol Version 4, Src: 100.65.0.101, Dst: 20.112.250.133
> Transmission Control Protocol, Src Port: 39286, Dst Port: 443, Seq: 1379, Ack: 1, Len: 525
> [3 Reassembled TCP Segments (1903 bytes): #81(1378), #83(525), #84(525)]
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1898
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 1894
      > Version: TLS 1.2 (0x0303)
        Random: abab5877b95bdaf0dedb5877db0126cb94139de1de21b6acdcac84499eb31eef
        Session ID Length: 32
        Session ID: 05b0087f38936d5d3b166ee5c0c1e7b24659f6d7b5d68c3814c0448d2bdefceb
        Cipher Suites Length: 34
      > Cipher Suites (17 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 1787
      > Extension: server_name (len=23) name=www.sharepoint.com
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)
      > Extension: supported_groups (len=16)
      > Extension: ec_point_formats (len=2)
      > Extension: session_ticket (len=0)
      > Extension: application_layer_protocol_negotiation (len=14)
      > Extension: status_request (len=5)
      > Extension: delegated_credentials (len=10)
      > Extension: signed_certificate_timestamp (len=0)
      > Extension: key_share (len=1327) Unknown (4588), x25519, secp256r1
      > Extension: supported_versions (len=5) TLS 1.3, TLS 1.2
      > Extension: signature_algorithms (len=24)
      > Extension: psk_key_exchange_modes (len=2)
      > Extension: record_size_limit (len=2)
      > Extension: compress_certificate (len=7)
      > Extension: encrypted_client_hello (len=281)
```

The packet capture output of a client hello message is shown.

You are updating a firewall policy that includes SSL certificate inspection. You are capturing packets from the traffic passing through this firewall policy.

Which two statements about the packet capture are correct? (Choose two.)

A. You can effectively apply an antivirus security profile to this traffic.

B. You can effectively apply a web filtering profile to this traffic.

C. The subject alternative name (SAN) is necessary to apply security profiles.

D. The client supports only TLS versions 1.2 and 1.3.

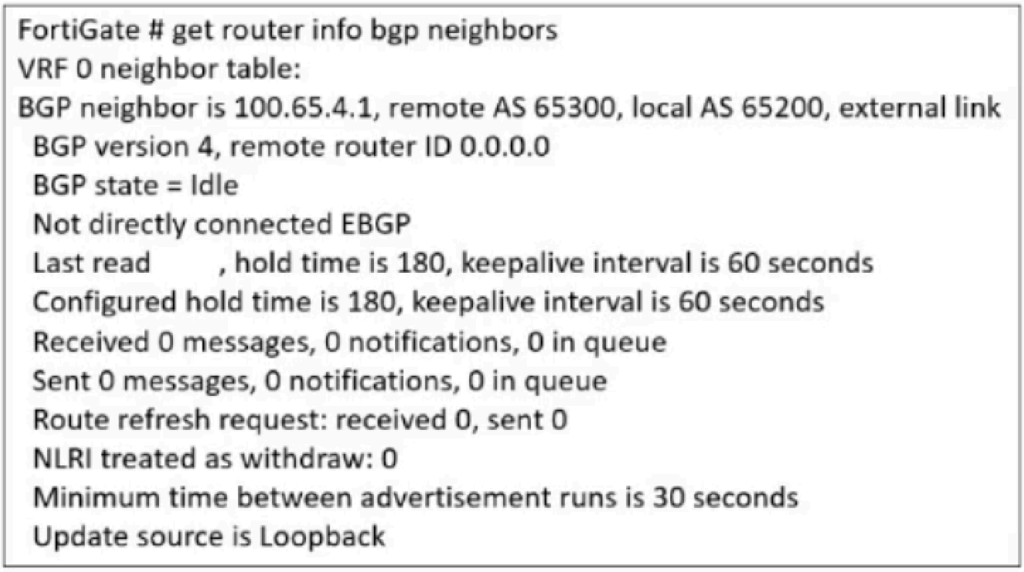
Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #17 Topic 1

Refer to the exhibit.

The status of a new BGP configuration on FortiGate is shown.



```
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
```

Based on the output shown in the exhibit, which configuration should you consider next?

A. Contact the remote peer administrator to enable BGP.

B. Configure a static route to 100.65.4.1.

C. Enable ebgp-multipath.

D. Enable ebgp-enforce-multihop.

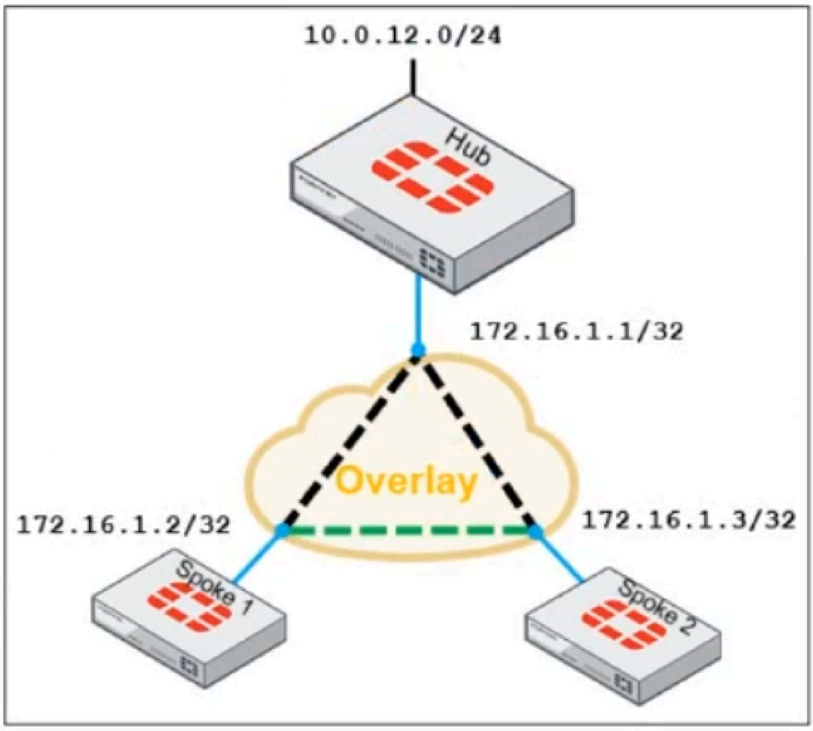
Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

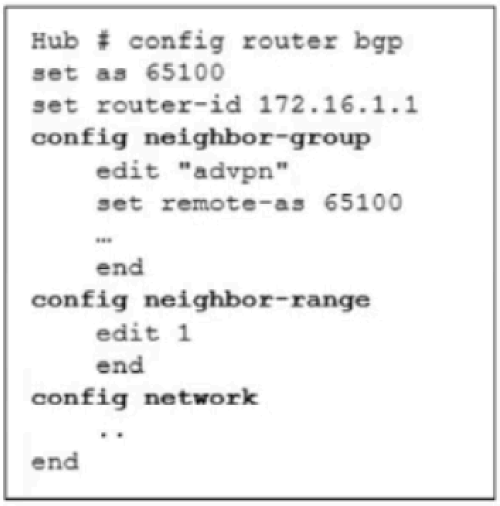
Question #18 *Topic 1*

Refer to the exhibits.

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
```

The ADVPN network topology and partial BGP configuration are shown.

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

A. set prefix 10.0.12.0 255.255.255.0

B. set route-reflector-client enable

C. set neighbor-group advpn

D. set prefix 172.16.1.0 255.255.255.0

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!