Fortinet

Exam Questions FCSS_EFW_AD-7.4

FCSS - Enterprise Firewall 7.4 Administrator

NEW QUESTION 1
An administrator must enable direct communication between multiple spokes in a company's network. Each spoke has more than one internet connection.
The requirement is for the spokes to connect directly without passing through the hub, and for the links to automatically switch to the best available connection.
How can this automatic detection and optimal link utilization between spokes be achieved?

A. Set up OSPF routing over static VPN tunnels between spokes.
B. Utilize ADVPN 2.0 to facilitate dynamic direct tunnels and automatic link optimization.
C. Establish static VPN tunnels between spokes with predefined backup routes.
D. Implement SD-WAN policies at the hub to manage spoke link quality.

Answer: B

Explanation:
ADVPN (Auto-Discovery VPN) 2.0is the optimal solution for enablingdirect spoke-to- spoke communicationwithout passing through the hub, while also allowingautomatic link selectionbased on quality metrics.
Dynamic Direct Tunnels:
ADVPN 2.0 allowsspokes to establish direct IPsec tunnels dynamicallybased on traffic patterns, reducing latency and improving performance.
Unlike static VPNs, spokes do not need to pre-configure tunnels for each other.
Automatic Link Optimization:
ADVPN 2.0monitors the qualityof multiple internet connections on each spoke.
It automatically switches to the best available connection when the primary linkdegrades or fails.
This is achieved by dynamically adjusting BGP-based routing or leveraging SD-WAN integration.

NEW QUESTION 2
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

Explanation:
TheFortinet FGSP (FortiGate Session Life Support Protocol) clusterallows session synchronization betweentwo FortiGate devicesto provide seamless failover.
However, ICMP (ping) is a connectionless protocol, and by default, FortiGate does not synchronize connectionless sessions unless explicitly enabled.
In the exhibit:
The commandget system session list | grep icmponFortiGate_Breturnsno output, meaning that ICMP sessions arenot being synchronizedfrom FortiGate_A.
Ifsession-pickup-connectionlessis disabled,FortiGate_B will not receive ICMP sessions, causingpacket lossduring failover.

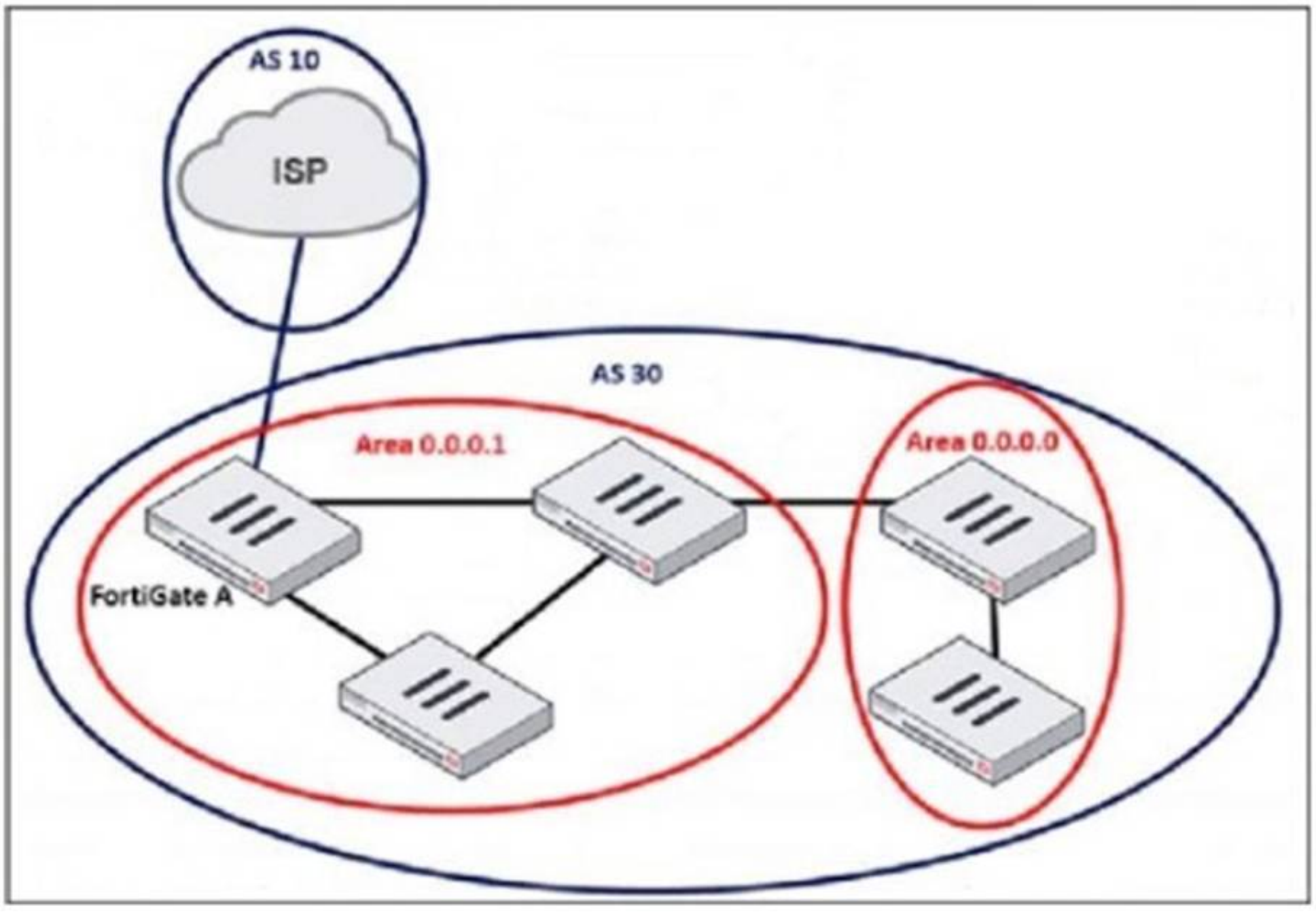
NEW QUESTION 3
Which two statements about IKEv2 are true if an administrator decides to implement IKEv2 in the VPN topology? (Choose two.)

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

Explanation:
IKEv2 (Internet Key Exchange version 2) is an improvement over IKEv1, offering enhanced security, efficiency, and flexibility in VPN configurations.
It includes stronger Diffie-Hellman (DH) groups, such as Elliptic Curve (ECP) groups. IKEv2 supports stronger cryptographic algorithms, includingElliptic Curve Diffie- Hellman (ECDH)groups such asECP256 and ECP384, providing improved security compared to IKEv1.
It supports the extensible authentication protocol (EAP).
IKEv2 natively supports EAP authentication, which allows integration with external authentication mechanisms such asRADIUS, certificates, and smart cards. This is particularly useful forremote access VPNswhere user authentication must be flexible and secure.

NEW QUESTION 4
Refer to the exhibit, which shows an enterprise network connected to an internet service provider.



The administrator must configure the BGP section of FortiGate A to give internet access to the enterprise network.
Which command must the administrator use to establish a connection with the internet service provider?

A. config neighbor
B. config redistribute bgp
C. config router route-map
D. config redistribute ospf

Answer: A

Explanation:
InBGP (Border Gateway Protocol), aneighbor (peer) configurationis required to establish a connection between two BGP routers. SinceFortiGate A is connecting to the ISP (Autonomous System 10) from AS 30, the administrator must define theISP's BGP router as a neighbor.
Theconfig neighborcommand is used to: Define the ISP's IP address as a BGP peer Specify the remote AS (AS 10 in this case)
Allow BGP route exchanges between FortiGate A and the ISP

NEW QUESTION 5
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 minimizeCPU and RAM usagewhile still enforcingsecurity features like web filtering and application control,SSL certificate inspection modeis the best choice.
SSL certificate inspectionallows FortiGate to inspectonly the SSL/TLS handshake, including theServer Name Indication (SNI) and certificate details, without decrypting the full encrypted payload.
This enables features likeweb filtering and application controlbecause FortiGate can determine thedestination website or applicationbased onSNI and certificate information.
Itsignificantly reduces system loadcompared tofull SSL inspection, which requires full decryption and re-encryption of traffic.

NEW QUESTION 6
Refer to the exhibit, which contains a partial VPN configuration.

```
config vpn ipsec phase1-interface
edit tunnel
set type dynamic
set interface "port1"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 aes256-sha256
set dpd on-idle
set add-route enable
set psksecret fortinet
next
end
```

What can you conclude from this VPN IPsec phase 1 configuration?

A. This configuration is the best for networks with regular traffic intervals, providing a balance between connectivity assurance and resource utilization.
B. Peer IDs are unencrypted and exposed, creating a security risk.
C. FortiGate will not add a route to its routing or forwarding information base when the dynamic tunnel is negotiated.
D. A separate interface is created for each dial-up tunnel, which can be slower and more resource intensive, especially in large networks.

Answer: A

Explanation:
ThisIPsec Phase 1 configurationdefines adynamicVPN tunnel that can accept connections from multiple peers. The settings chosen here suggest a configuration optimized fornetworks with intermittent traffic patternswhile ensuring resources are used efficiently.
Key configurations and their impact:
set type dynamic This allows multiple peers to establish connections dynamically without needing predefined IP addresses.
set ike-version 2 UsesIKEv2, which is more efficient and supports features like EAP
authentication and reduced rekeying overhead.
set dpd on-idle Dead Peer Detection (DPD) is triggeredonly when the tunnel is idle, reducing unnecessary keep-alive packets and improving resource utilization.
set add-route enable FortiGate automatically adds the route to the routing table when the tunnel is established, ensuring connectivity when needed.
set proposal aes128-sha256 aes256-sha256 Uses strong encryption and hashing algorithms, ensuring a secure connection.
set keylife 28800 Sets alonger key lifetime(8 hours), reducing the frequency of rekeying, which is beneficial for stable connections.
BecauseDPD is set to on-idle, the tunnel will not constantly send keep-alive messages but will still ensure connectivity when traffic is detected. This makes the configuration ideal fornetworks with regular but non-continuous traffic, balancing security and resource efficiency.

NEW QUESTION 7
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:
Thebest wayto block outdated SSL/TLS versions is toconfigure the SSL/SSH inspection profileto enforce aminimum SSL/TLS versionand disable weak SSL versions.
By setting theminimum allowed SSL versionin theHTTPS settings of the SSL/SSH inspection profile, FortiGate will:

Block any connection usingoutdated SSL/TLS versions(such as SSLv3, TLS 1.0, or TLS 1.1).
Enforce secure communication usingonly strong SSL/TLS versions(such as TLS 1.2 or TLS 1.3).
Protect users fromman-in-the-middle (MITM) and downgrade attacksthat exploit weak encryption.

NEW QUESTION 8
An administrator is designing an ADVPN network for a large enterprise with spokes that have varying numbers of internet links. They want to avoid a high number of routes and peer connections at the hub.
Which method should be used to simplify routing and peer management?

A. Deploy a full-mesh VPN topology to eliminate hub dependency.
B. Implement static routing over IPsec interfaces for each spoke.
C. Use a dynamic routing protocol using loopback interfaces to streamline peers and routes.
D. Establish a traditional hub-and-spoke VPN topology with policy routes.

Answer: C

Explanation:
When designing anADVPN (Auto-Discovery VPN) networkfor alarge enterprisewith spokes that havevarying numbers of internet links, the main challenge is tominimize the number of peer connections and routesat the hub while maintainingscalability and efficiency.
Using a dynamic routing protocol (such as BGP or OSPF) with loopback interfaces helps in several ways:
Reduces the number of peer connectionsat the hub byusing a single loopback address per spokeinstead of individual physical interfaces.
Enables simplified route advertisementby dynamically learning and propagating routes instead of manually configuring static routes.
Supports multiple internet links per spokeefficiently, as dynamic routing can automatically adjust to the best available path.
Allows seamless failoverif a spoke??s internet link fails, ensuring continuous connectivity.

NEW QUESTION 9
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

Explanation:
When usingIPsec VPNsandVXLAN, additional headers are added to packets, which can exceed thedefault 1500-byte MTU. This can lead tofragmentation issues, dropped packets, or degraded performance.
To resolve this, theMTU (Maximum Transmission Unit)should be adjustedonly if all devices in the network path support it. Otherwise, some devices may still drop or fragment packets, leading to continued issues.
Why adjusting MTU helps:
VXLAN adds a 50-byte overheadto packets.
IPsec adds additional encapsulation(ESP, GRE, etc.), increasing the packet size.
If packets exceed the MTU, they may befragmented or dropped, causing intermittent connectivity issues.
Lowering the MTU on interfaces ensurespackets stay within the supported size limit across all network devices.

NEW QUESTION 10
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 inIPsec Phase 2mean thatno specific traffic selectors (subnets) are defined, allowingany traffic to be encryptedthrough the VPN tunnel. This can cause unintended traffic forwarding issuesand disrupt network operations.
To prevent this from happening during future migrations:
Using routing protocolsensures thatonly 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 selectorsavoids the problem of encrypting all traffic by explicitly stating the allowed source and destination subnets. This prevents the tunnel from affecting unrelated network traffic.

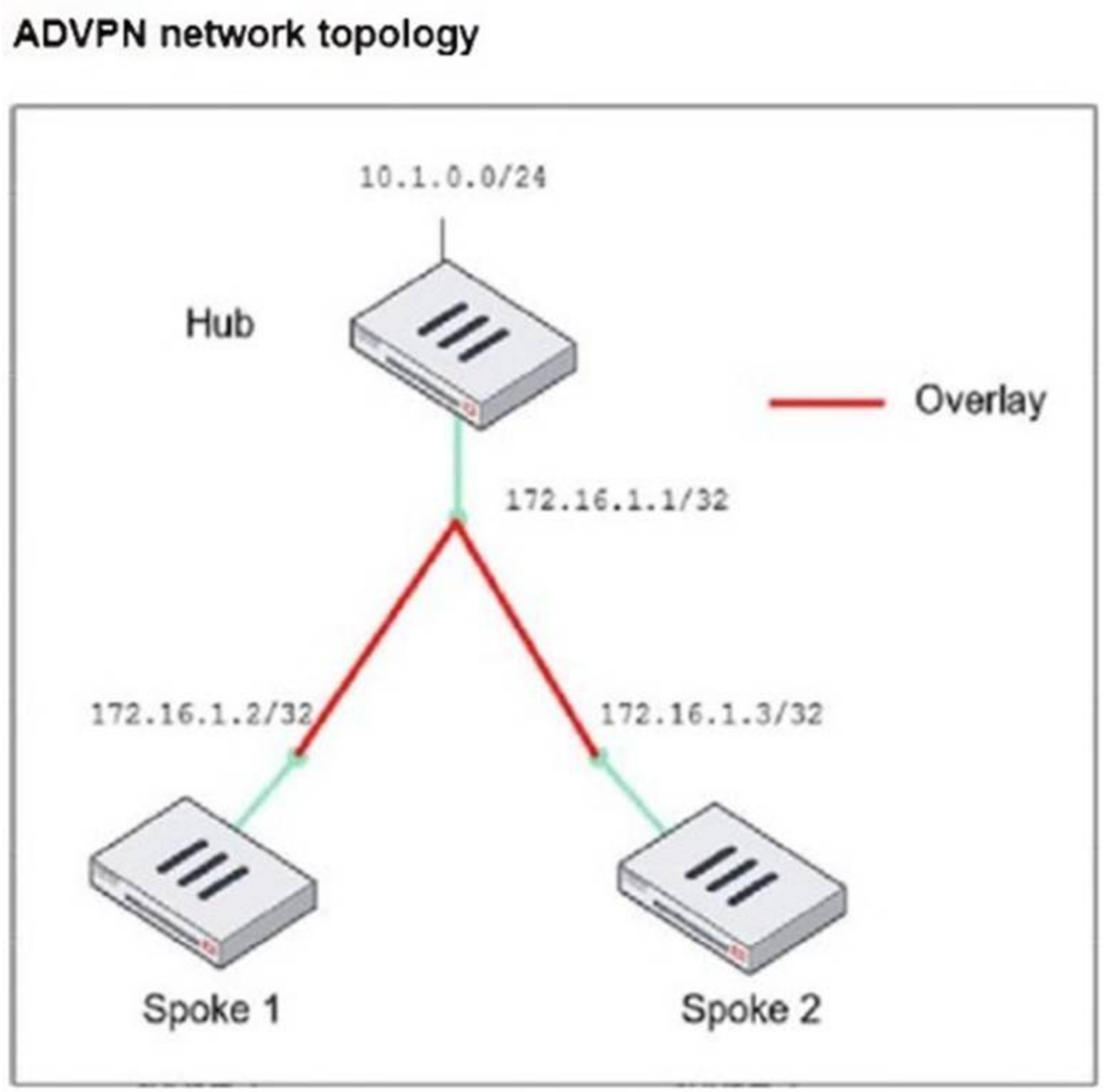
NEW QUESTION 10
A company's guest internet policy, operating in proxy mode, blocks access to Artificial Intelligence Technology sites using FortiGuard. However, a guest user accessed a page in this category using port 8443.
Which configuration changes are required for FortiGate to analyze HTTPS traffic on nonstandard ports like 8443 when full SSL inspection is active in the guest policy?

A. Add a URL wildcard domain to the website CA certificate and use it in the SSL/SSH Inspection Profile.
B. In the Protocol Port Mapping section of the SSL/SSH Inspection Profile, enter 443, 8443 to analyze both standard (443) and non-standard (8443) HTTPS ports.
C. To analyze nonstandard ports in web filter profiles, use TLSv1.3 in the SSL/SSH Inspection Profile.
D. Administrators can block traffic on nonstandard ports by enabling the SNI check in the SSL/SSH Inspection Profile.

Answer: B

Explanation:
When FortiGate is operating inproxy modewithfull SSL inspection enabled, it inspects encrypted HTTPS traffic by default onport 443. However, some websites may usenon- standard HTTPS ports(such as 8443), which FortiGate does not inspect unless explicitly configured.
To ensure that FortiGate inspects HTTPS traffic onport 8443, administrators must manually add port 8443in theProtocol Port Mappingsection of theSSL/SSH Inspection Profile. This allows FortiGate to treat HTTPS traffic on port 8443 the same as traffic on port 443, enabling proper inspection and enforcement ofFortiGuard category-based web filtering.

NEW QUESTION 15
Refer to the exhibit, which shows the ADVPN network topology and partial BGP configuration.



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

Explanation:
In the given ADVPN (Auto-Discovery VPN) topology, BGP is being used to dynamically establish routes between spokes. The neighbor-range configuration is crucial for simplifying BGP peer setup by automatically assigning neighbors based on their IP range.
set neighbor-group advpn
Theneighbor-groupparameter is used to apply pre-defined settings (such as AS number) to dynamically discovered BGP neighbors.
Theadvpnneighbor-group is already defined in the configuration, and assigning it to the neighbor-range ensures consistent BGP settings for all spoke neighbors.
set prefix 172.16.1.0 255.255.255.0
This command allowsdynamic BGP peer discoveryby defining a range of potential neighbor IPs (172.16.1.1 - 172.16.1.255).
Sinceeach spoke has a unique /32 IPwithin this subnet, this ensures that any spoke within the172.16.1.0/24range can automatically establish a BGP session with the hub.

NEW QUESTION 16
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
```

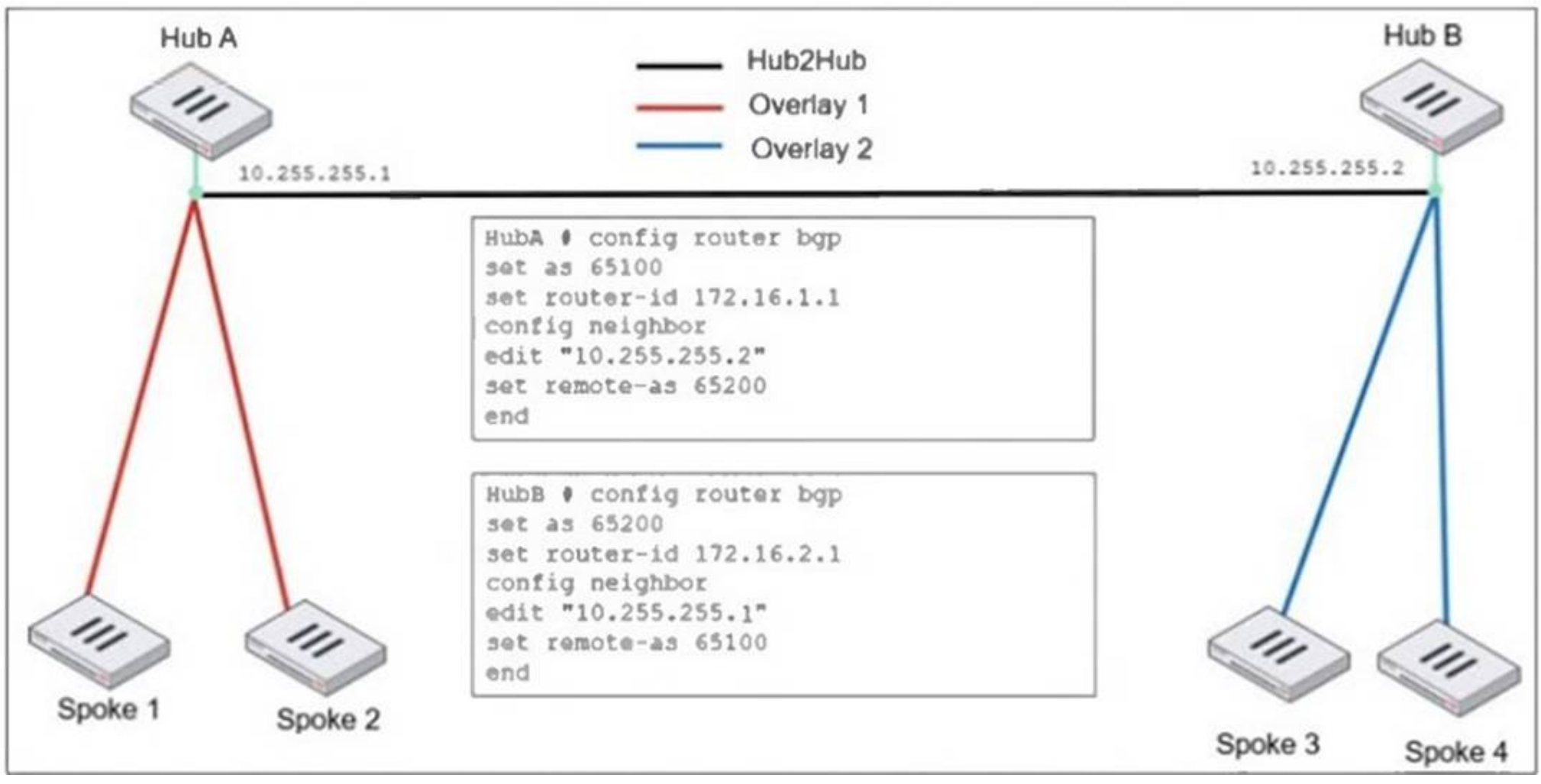
An administrator is extensively using IPsec on FortiGate. Many tunnels show information similar to the output shown in the exhibit.
What can the administrator conclude?

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

Explanation:
The diagnose vpn tunnel list name Hub2Spoke1 command output provides key information about the offloading status of an IPsec VPN tunnel to the Network Processing Unit (NPU). npu_flag=20:
This flag indicates that both inbound and outbound IPsec Security Associations (SAs) have been offloaded to the NPU, meaning the VPN traffic is processed in hardware instead of the CPU.
npu_rgwy=10.10.2.2 and npu_lgwy=10.10.1.1:
These IPs represent the remote gateway (rgwy) and local gateway (lgwy), confirming that the tunnel is successfully offloaded.
npu_selid=1:
This value means the session selector for the NPU offloaded SA is active.
Since both inbound and outbound SAs are offloaded, the administrator can conclude that the FortiGate NPU is handling IPsec encryption and decryption efficiently, reducing CPU load and improving VPN performance.

NEW QUESTION 17
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 thisADVPN (Auto-Discovery VPN) network, there are two hubs (Hub A and Hub B) connected viaEBGP, whileIBGPis 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.

NEW QUESTION 21
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:
Whenstandardizing the deployment of FortiGate devices across branchesusing FortiManager, thebest practiceis to usemetadata variables. This allows fordynamic interface configurationwhile maintaining asingle, consistent policy packagefor all branches.
Metadata variablesin FortiManager enableinterface roles and configurations to be dynamically assignedbased on the specific FortiGate device.
This ensuresscalabilityandconsistent security policy enforcementacross all branches without manually adjusting interface settings for each device.
When a new branch FortiGate is deployed, metadata variables automaticallymap to the correct physical interfaces, reducing manual configuration errors.

NEW QUESTION 25
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

Explanation:
Whenadding an additional FortiGateto an enterprise network that is already reaching itsresource limits, the goal is to distribute traffic efficiently and ensurehigh availability.
FGSP (FortiGate Session Life Support Protocol) with external load balancers
FGSP allowssession-aware load balancingbetween multiple FortiGate units without
requiring them to be in an HA (High Availability) cluster.
Withexternal load balancers, incoming traffic isevenly distributedacross multiple FortiGate devices.
This approach is useful forscaling outtraffic handling capacity while ensuring that sessions remainsynchronizedbetween firewalls.
FGSP is effectivewhen stateful failover is requiredbut without the constraints of traditional HA.
FGCP (FortiGate Clustering Protocol) in active-active mode and with switches FGCPactive-active modeenables multiple FortiGate devices toshare traffic loads, increasing throughput and efficiency.
Active-active mode is suitable forbalancing UTM processingacross multiple FortiGates, making it ideal whenresource limits are a concern.
Usingswitchesensures redundancy and avoids single points of failure in the network.
This mode is commonly used inenterprise networkswhere bothscalability and redundancyare required.

NEW QUESTION 29
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.

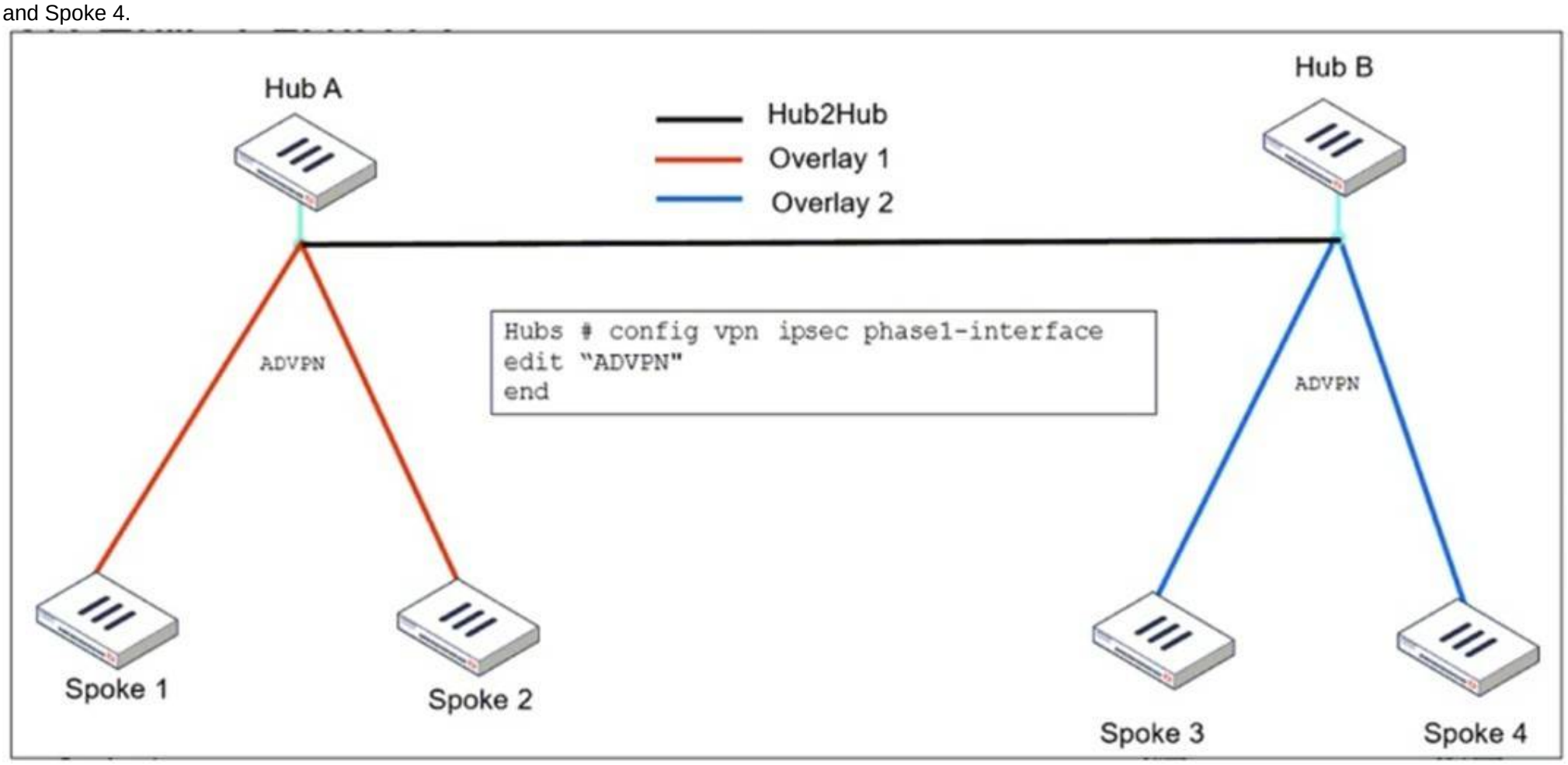
Which statement on this FortiGate device is correct?

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 theOSPF status output, the key information is:
"This router is an ASBR" This means the FortiGate is acting as anAutonomous System Boundary Router (ASBR).
AnASBRis responsible for injectingexternal routing informationinto OSPF from another routing protocol (such as BGP, static routes, or connected networks).

NEW QUESTION 34
Refer to the exhibit, which shows theADVPNIPsec 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 theADVPNtunnels?

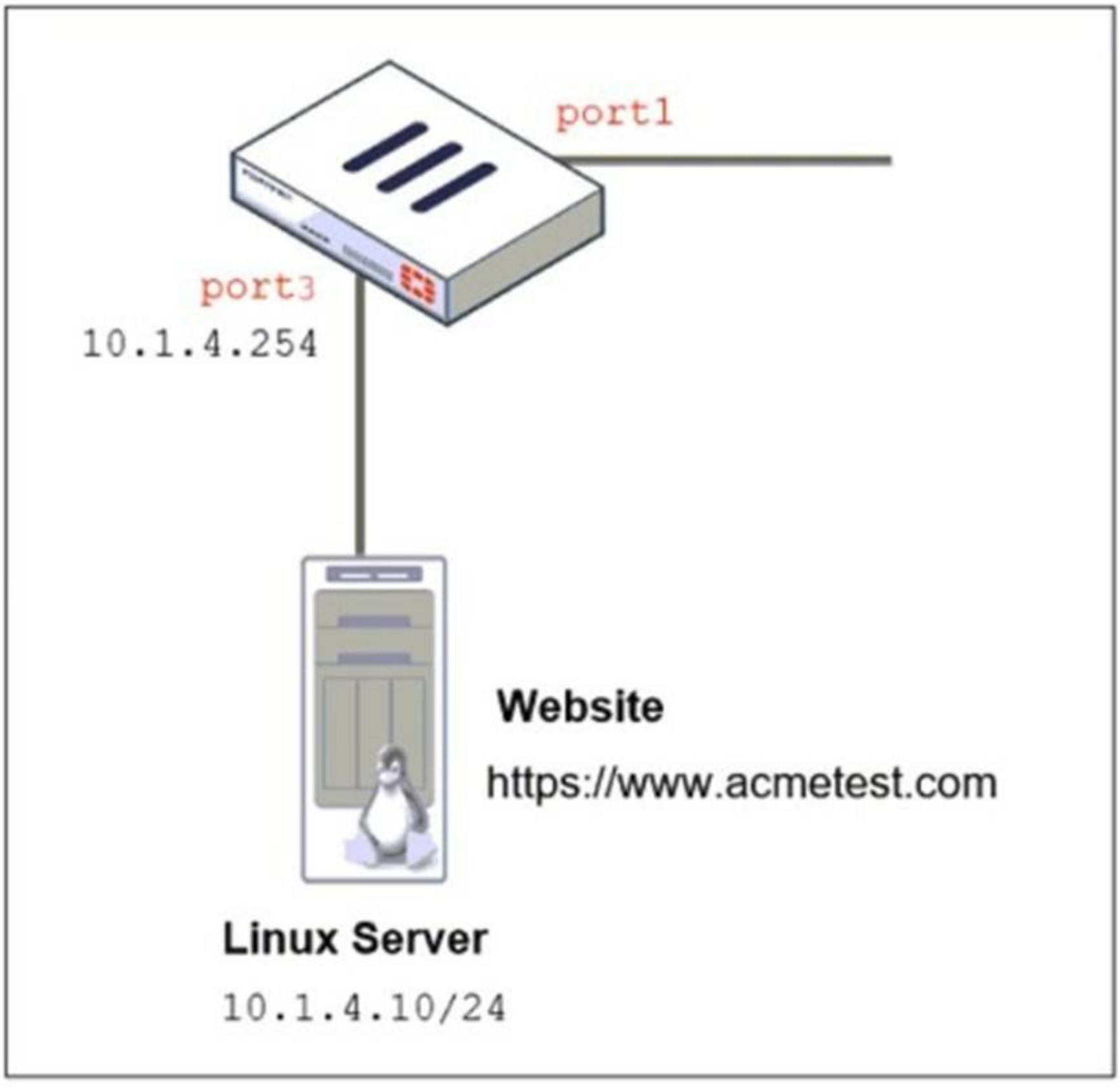
A. set auto-discovery-sender enable and set network-id x
B. set auto-discovery-forwarder enable and set remote-as x
C. set auto-discovery-crossover enable and set enforce-multihop enable
D. set auto-discovery-receiver enable and set npu-offload enable

Answer: C

Explanation:
When configuringADVPN (Auto-Discovery VPN)to connectoverlay networks across different hubs using IBGP and EBGP, special configurations are required to allow spokes from different overlay networks to dynamically establish tunnels.
set auto-discovery-crossover enable
Thisallows cross-hub tunnel discoveryin an ADVPN deployment where multiple hubs are used.
SinceHub A and Hub Bbelong to different overlays, enablingcrossover discoveryensures that spokes from one overlay can dynamically create direct tunnels to spokes in the other overlay when needed.
set enforce-multihop enable
This setting ensures thatBGP peers using loopback interfacescan establish connectivityeven if they are not directly connected.
Multihop BGP sessionsare required when usingloopback addresses as BGP peer sourcesbecause the connection might need to traverse multiple routers before reaching the BGP neighbor.
This is especially useful inADVPN deployments with multiple hubs, where routes might
need to cross from one hub to another.

NEW QUESTION 36
Refer to the exhibits. The exhibits show a network topology, a firewall policy, and an SSL/SSH inspection profile configuration.

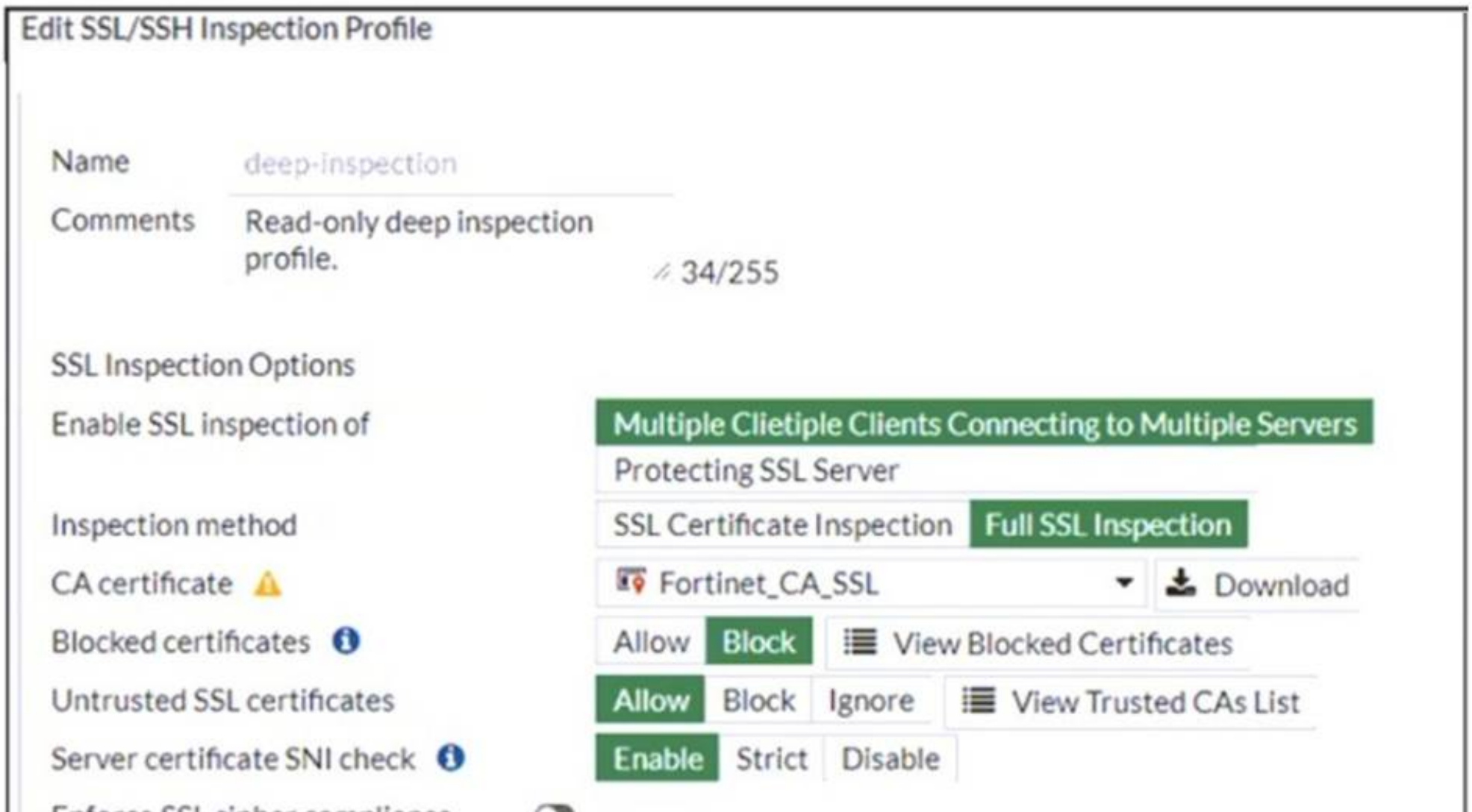
Network Topology



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



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

Explanation:
The FortiGateSSL/SSH inspection profileis configured forFull SSL Inspection, which is necessary to analyze encrypted HTTPS traffic. However, the firewallpolicy is protecting an SSL server (the Linux server hosting the website), and currently, the SSL/SSH profileonly applies to client-side SSL inspection.
To detect HTTPS-based attacks targeting the Linux server:
FortiGate must act as an SSL intermediaryto inspect encrypted traffic destined for the web server.
The administratormust upload the SSL certificate of the Linux web serverto FortiGate so that theserver-side SSL inspectioncan decrypt incoming HTTPS traffic before analyzing it.

NEW QUESTION 39
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?

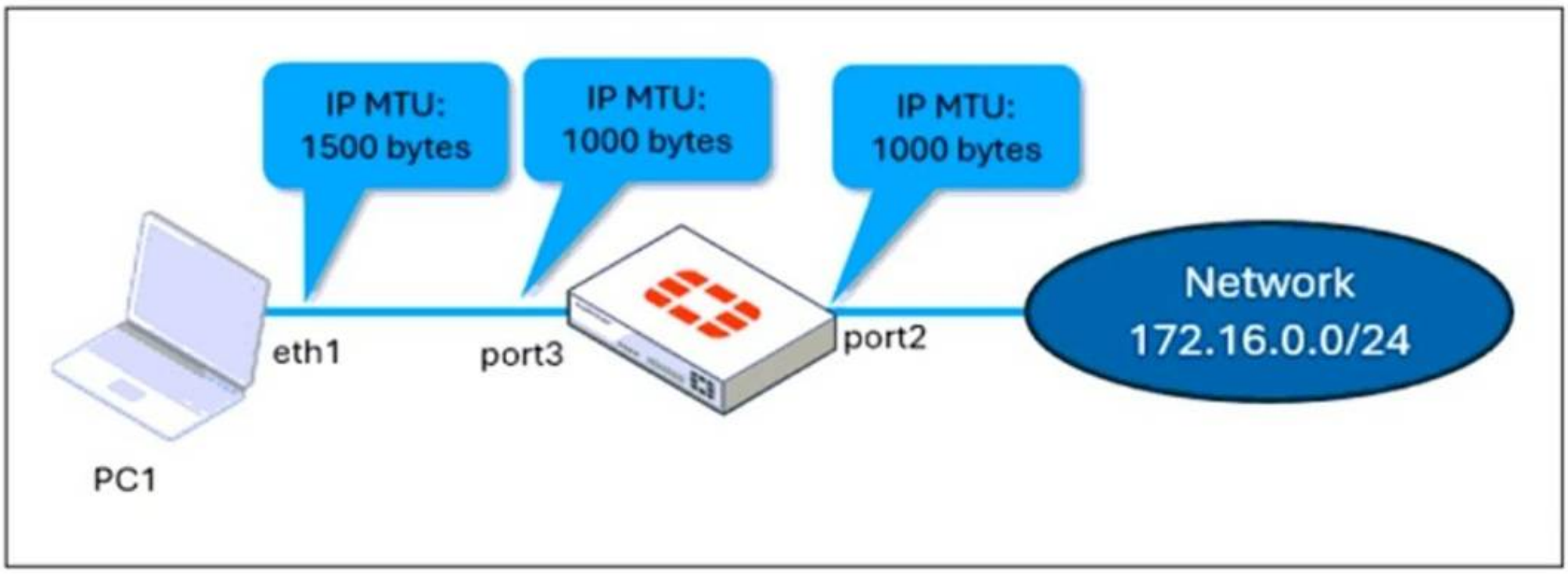
A. The administrator must enable reputable websites to allow only SSL/TLS websites rated by FortiGuard web filter.
B. The administrator must enable URL extraction from SNI on the SSL certificate inspection to ensure the TLS three-way handshake is correctly analyzed by FortiGate.
C. The administrator 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

Explanation:
FortiGate, like other security appliances, cannot analyze encrypted HTTPS traffic unless it decryptsit first. Ifonly certificate inspectionis enabled, FortiGate can see the certificate details (such as the domain and issuer) butcannot inspect the actual web content.
To fully analyze the traffic and detect potential malware threats:
Full SSL inspection (Deep Packet Inspection)must be enabled in theSSL/SSH Inspection Profile.
This allows FortiGate todecrypt the HTTPS traffic, inspect the content, and then re-Without full SSL inspection, threats embedded in encrypted traffic may go undetected.

NEW QUESTION 41
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),
```

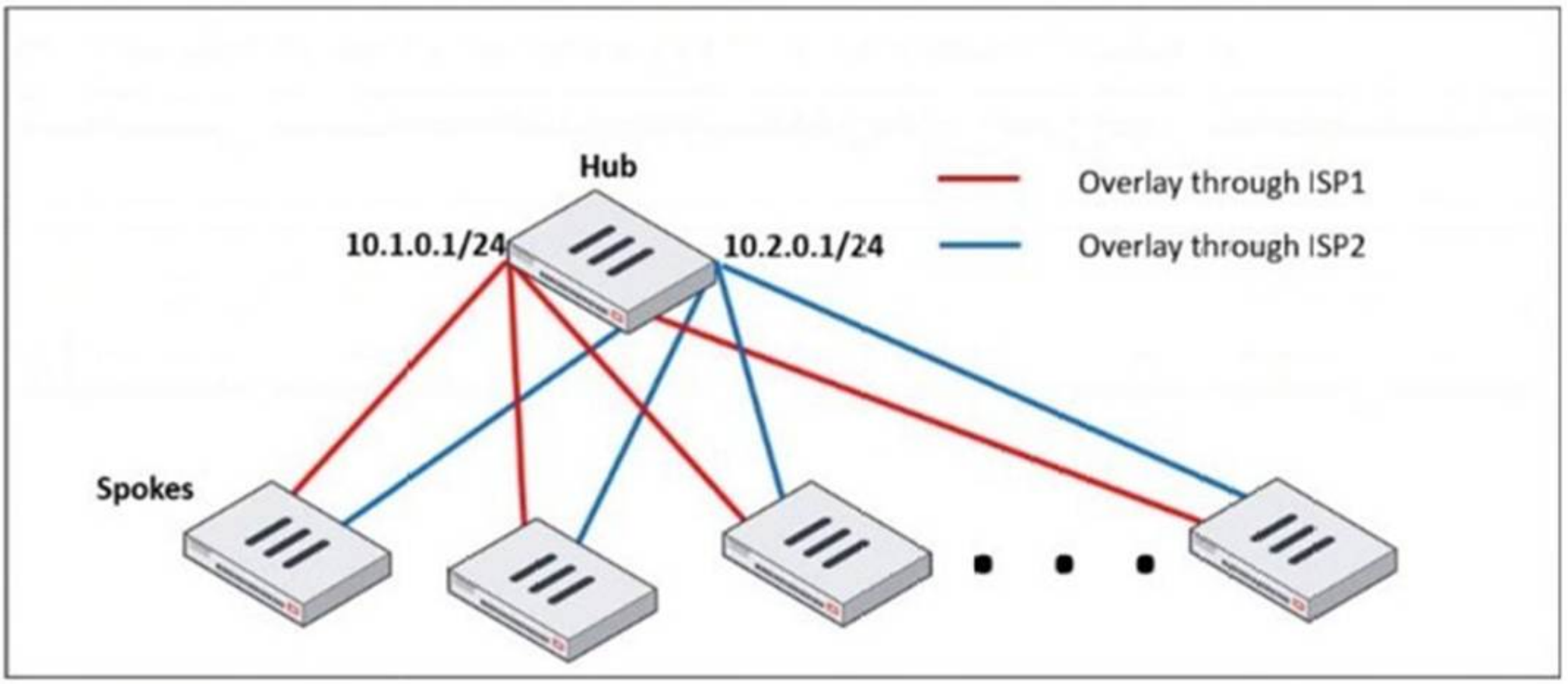
with FortiGate interfaces set to an MTU of1000bytes, and the results of PC1 pinging
server172.16.0.254are shown.
Why is the user in Windows PC1 unable to ping server172.16.0.254and is seeing the message:Packet needs to be fragmented but DF set?

A. Option ip.flags.mf must be set to enable on FortiGat
B. The user has to adjust the ping MTU to 1000 to succeed.
C. Fragmented packets must be encrypte
D. To connect any application successfully, the user must install the Fortinet_CA certificate in the Microsoft Management Console.
E. FortiGate honors the do not fragment bit and the packets are droppe
F. The user has to adjust the ping MTU to 972 to succeed.
G. The user must trigger different traffic because path MTU discovery techniques do not recognize ICMP payloads.

Answer: C

Explanation:
The issue occurs because FortiGate enforces the "do not fragment" (DF) bit in the packet, and the packet size exceeds the MTU of the network path. When the Windows PC1 (with an MTU of 1500 bytes) attempts to send a 1400-byte packet, the FortiGate interface (with an MTU of 1000 bytes) needs to fragment it. However, since the DF bit is set, FortiGate drops the packet instead of fragmenting it.
To resolve this, the user should adjust the ping packet size to fit within the path MTU. In this case, reducing the packet size to972 bytes(1000 bytes MTU minus 28 bytes for the IP and ICMP headers) should allow successful transmission.

NEW QUESTION 43
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

Explanation:
neighbor-group:
This command is used to group multipleBGP neighborswith the same configuration, reducing redundant configuration.
Instead of defining individual BGP settings for each spoke, the administrator can create a neighbor-groupand apply the same policies, reducing manual work.
neighbor-range:
This command allows the configuration ofa range of neighbor IPs dynamically, reducing the need to manually define each spoke neighbor.
It automatically addsBGP neighborsthat match a given prefix, simplifying deployment.

NEW QUESTION 46
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

Explanation:
TheInternet Service Database (ISDB)in FortiGate is used to enforce content filtering at Layer 3 (Network Layer) and Layer 4 (Transport Layer)of the OSI model by identifying applications based on theirpredefined IP addresses and ports.
FortiGate has a predefined list of all IPs and ports for specific applications downloaded from FortiGuard:
FortiGate retrieves and updates apredefined listof IPs and ports for different internet services fromFortiGuard.
This allows FortiGate to block specific services atLayer 3 and Layer 4without requiring deep packet inspection.
The ISDB blocks the IP addresses and ports of an application predefined by FortiGuard:
ISDB works by matching traffic to knownIP addresses and portsof categorized services. When an application or service is blocked, FortiGate prevents communication bydenying traffic based on its destination IP and port number.

NEW QUESTION 47
What does the command set forward-domain <domain_ID> in a transparent VDOM interface do?

A. It configures the interface to prioritize traffic based on the domain ID, enhancing quality of service for specified VLANs.
B. It isolates traffic within a specific VLAN by assigning a broadcast domain to an interfacebased on the VLAN ID.
C. It restricts the interface to managing traffic only from the specified VLAN, effectively segregating network traffic.
D. It assigns a unique domain ID to the interface, allowing it to operate across multiple VLANs within the same VDOM.

Answer: B

Explanation:
In atransparent mode Virtual Domain (VDOM)configuration, FortiGate operates as a
Layer 2 bridgerather than performing Layer 3 routing. Theset forward-domain
<domain_ID>command is used to control how traffic is forwarded between interfaces within the sametransparent VDOM.
Aforward-domainacts as abroadcast domain, meaning only interfaces with thesame forward-domain IDcan exchange traffic. This setting is commonly used

toseparate different VLANs or network segmentswithin the transparent VDOM while still allowing FortiGate to apply security policies.

NEW QUESTION 50
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 route172.16.1.248/30on 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

Explanation:
FortiGate_A and FortiGate_B are in thesame autonomous system (AS), andFortiGate_Adoesnot currently have route 172.16.1.248/30in its routing table. However, FortiGate_B has this routeas a connected route.
To dynamically advertiseonly172.16.1.248/30 fromFortiGate_B to FortiGate_A, the administrator must configure aBGP route map outonFortiGate_Bthat specifically permitsonlythis prefix.
A BGP route map out on FortiGate_Bcontrols which routes FortiGate_B advertises to FortiGate_A. If no filtering is applied, FortiGate_B might advertiseall BGP-learned and connected routes, which is not what the administrator wants. The route map should include aprefix-listthat explicitlyallows only172.16.1.248/30 and denies everything else.

NEW QUESTION 53
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

Explanation:
Thebest way to automate a firewall policyusing a daily updated list ofIP addressesis by using anexternal connector from Threat Feeds. This allows FortiGate to dynamically retrievereal-time threat intelligencefrom external sources and apply it directly to security policies.
By configuringThreat Feeds, the administrator can:
Automatically updatefirewall policies with the latest malicious IPs daily.
Block trafficfrom those IPs in real-time without manual intervention.
Integrate with FortiGuard, third-party threat intelligence sources, or custom feeds (CSV, STIX/TAXII, etc.).

NEW QUESTION 56
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

FCSS_EFW_AD-7.4 Practice Exam Features:

* FCSS_EFW_AD-7.4 Questions and Answers Updated Frequently

* FCSS_EFW_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_EFW_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_EFW_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year