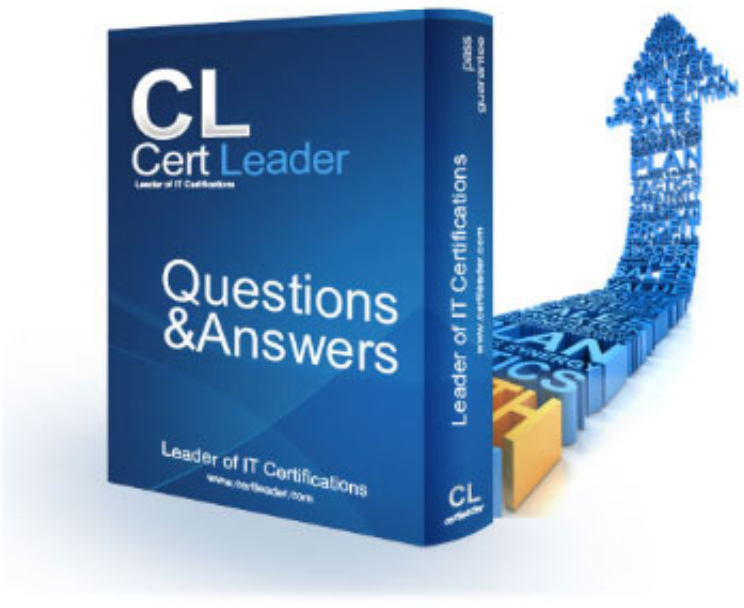
FCSS_EFW_AD-7.4 Dumps

FCSS - Enterprise Firewall 7.4 Administrator

https://www.certleader.com/FCSS_EFW_AD-7.4-dumps.html



NEW QUESTION 1
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

Explanation:
The MAC addresse0:23:ff:fc:00:86follows the format used in FortiGate High Availability (HA) clusters. When FortiGate devices are in an HA configuration, they use virtual MAC addresses for failover and redundancy purposes.
The suspicious packet is related to a cluster that has VDOMs enabled:FortiGate devices with Virtual Domains (VDOMs)enabled use specific MAC address ranges to differentiate HA-related traffic. This MAC address is likely part of that mechanism.
The suspicious packet is related to a cluster with a group-id value lower than 255: FortiGate HA clusters assign virtual MAC addresses based on thegroup ID. The last octet (00:86) corresponds to agroup IDthat isbelow 255, confirming this option.

NEW QUESTION 2
Refer to the exhibit, which shows a physical topology and a traffic log.

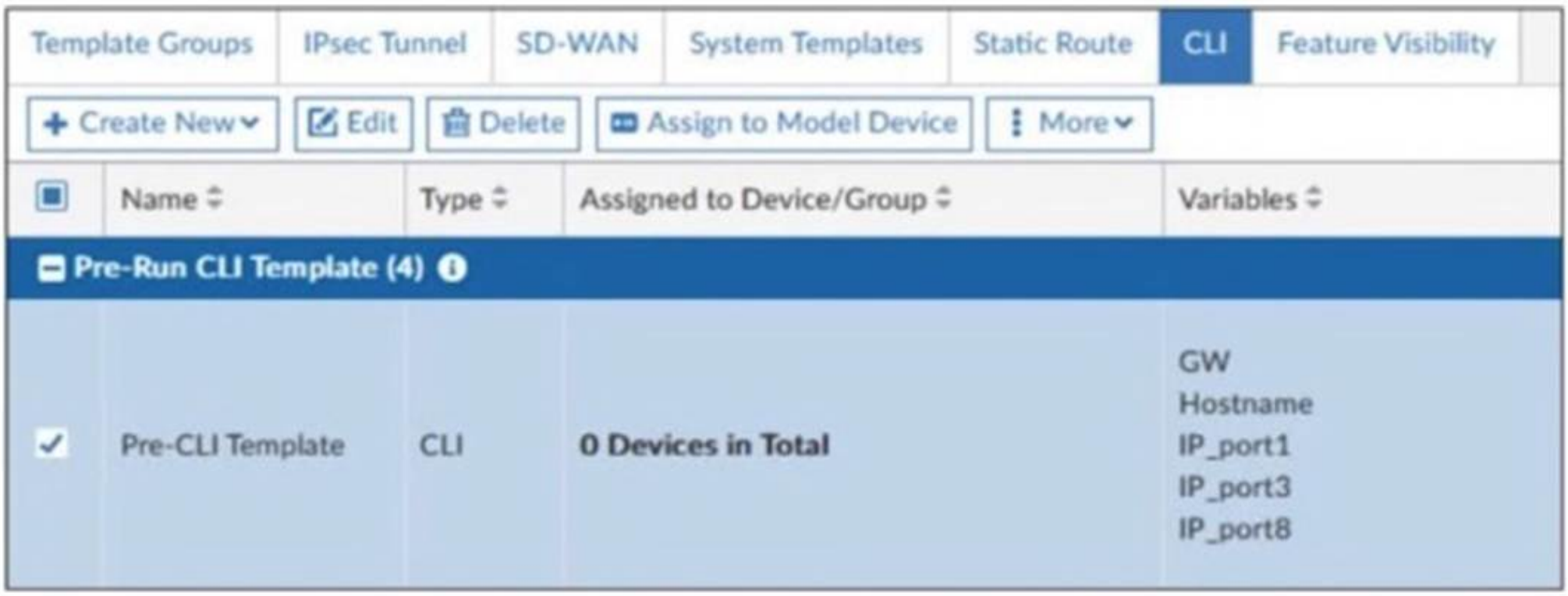
The administrator is checking on FortiAnalyzer traffic from the device with IP address10.1.10.1, located behind the FortiGate ISFW device.
The firewall policy in on the ISFW device does not have UTM enabled and the administrator is surprised to see a log with the actionMalware, as shown in the exhibit.
What are the two reasons FortiAnalyzer would display this log? (Choose two.)

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

Answer: BD

Explanation:
From the exhibit, ISFW is part of a Security Fabric environment with NGFW-1 as the Fabric Root. In this architecture, FortiGate devices share security intelligence, including logs and detected threats.
ISFW is in a Security Fabric environment:
Security Fabric allows devices like ISFW toreceive threat intelligencefrom NGFW-1, even if UTM is not enabled locally.
If NGFW-1 detects malware fromIP 10.1.10.1 to 89.238.73.97, this information can be propagated to ISFW and FortiAnalyzer.
The firewall policy in NGFW-1 has UTM enabled:
Even thoughISFW does not have UTM enabled, NGFW-1 (which sits between ISFW and the external network)does have UTM enabledand is scanning traffic.
Since NGFW-1 detects malware in the session, it logs the event, which is then sent to FortiAnalyzer.

NEW QUESTION 3
Refer to the exhibit.
A pre-run CLI template that is used in zero-touch provisioning (ZTP) and low-touch provisioning (LTP) with FortiManager is shown.



The template is not assigned even though the configuration has already been installed on FortiGate.
What is true about this scenario?

A. The administrator did not assign the template correctly when adding the model device because pre-CLI templates remain permanently assigned to the firewall
B. Pre-run CLI templates are automatically unassigned after their initial installation
C. Pre-run CLI templates for ZTP and LTP must be unassigned manually after the first installation to avoid conflicting error objects when importing a policy package
D. The administrator must use post-run CLI templates that are designed for ZTP and LTP

Answer: B

Explanation:
InFortiManager,pre-run CLI templatesare used inZero-Touch Provisioning (ZTP)and Low-Touch Provisioning (LTP)to configure a FortiGate devicebeforeit is fully managed by FortiManager.
These templatesapply configurationswhen a device is initially provisioned.Once the pre- run CLI template is executed, FortiManagerautomatically unassignsit from the device because it isnot meant to persistlike other policy configurations. This prevents conflicts and ensures that the FortiGate configuration isnot repeatedly appliedafter the initial setup.

NEW QUESTION 4
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 5
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
```

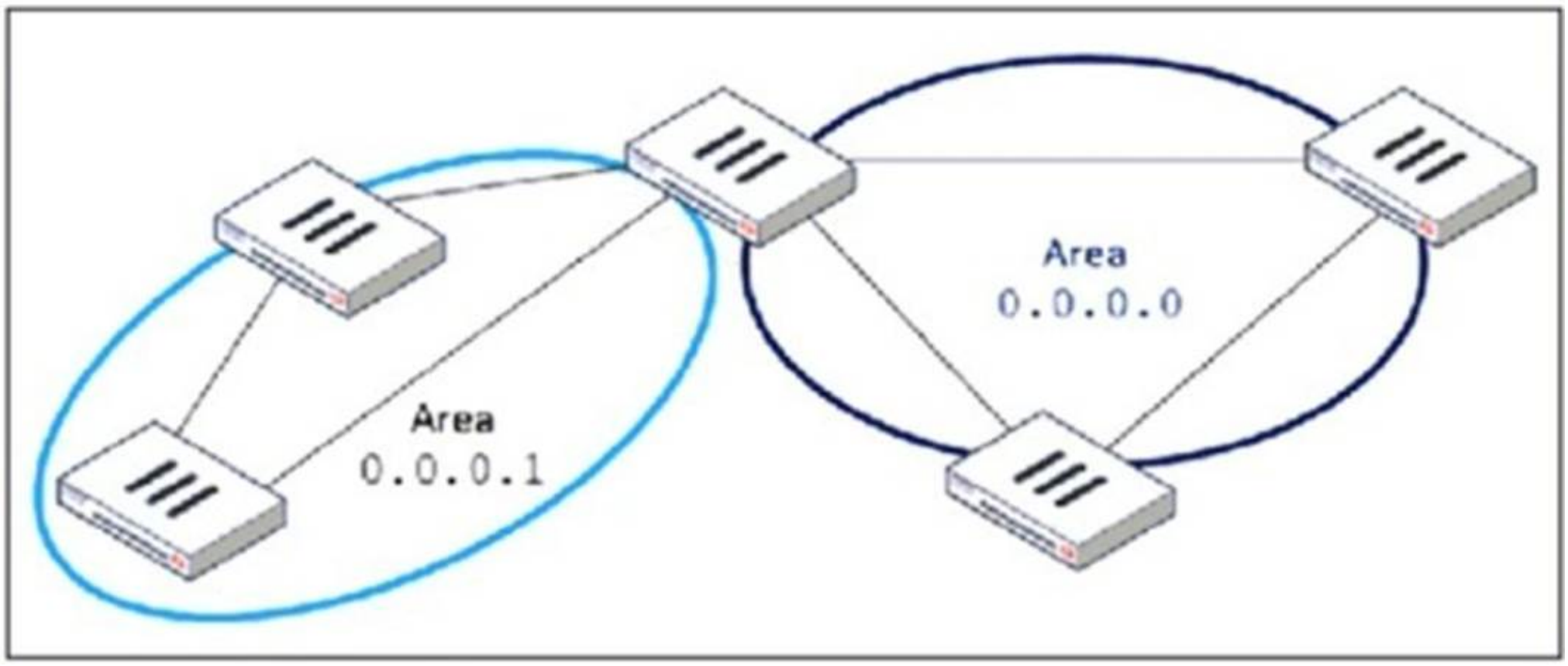
What can you conclude from this VPN IPsec phase 1 configuration?

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 6
Refer to the exhibit, which shows an OSPF network.



Which configuration must the administrator apply to optimize the OSPF database?

A. Set a route map in the AS boundary FortiGate.
B. Set the area 0.0.0.1 to the type STUB in the area border FortiGate.
C. Set an access list in the AS boundary FortiGate.
D. Set the area 0.0.0.1 to the type NSSA in the area border FortiGate.

Answer: B

Explanation:
TheOSPF database optimizationis necessary to reduce unnecessary routing information and improve network performance. In the given topology,Area 0.0.0.1is a non-backbone area connected toArea 0.0.0.0 (the backbone area)through anArea Border Router (ABR).
To optimize OSPF in this scenario, configuringArea 0.0.0.1 as a Stub Areawill:
Reduce the size of the OSPF databaseby preventing external routes (from outside OSPF) from being injected into Area 0.0.0.1.
Allow only intra-area and inter-area routes, meaning routers in Area 0.0.0.1 will rely on a default routefor external destinations.
Improve convergence time and reduce router processing loadsince fewer LSAs (Link- State Advertisements) are exchanged.

NEW QUESTION 7
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 8
An administrator applied a block-all IPS profile for client and server targets to secure the server, but the database team reported the application stopped working immediately after.
How can an administrator apply IPS in a way that ensures it does not disrupt existing applications in the network?

A. Use an IPS profile with all signatures in monitor mode and verify patterns before blocking.
B. Limit the IPS profile to server targets only to avoid blocking connections from the server to clients.
C. Select flow mode in the IPS profile to accurately analyze application patterns.
D. Set the IPS profile signature action to default to discard all possible false positives.

Answer: A

Explanation:
Applying anaggressive IPS profilewithout prior testing candisrupt legitimate applicationsby incorrectly identifying normal traffic as malicious. To prevent disruptions while still monitoring for threats:
Enable IPS in "Monitor Mode" first:
This allows FortiGate tolog and analyzepotential threatswithout actively blockingtraffic. Administrators can review logs and fine-tune IPS signatures to minimize false positives before switching to blocking mode.

Verify and adjust signature patterns:
Some signatures might trigger unnecessary blocks for legitimate application traffic. By analyzing logs, administrators candisable or modifyspecific rules causing false positives.

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.

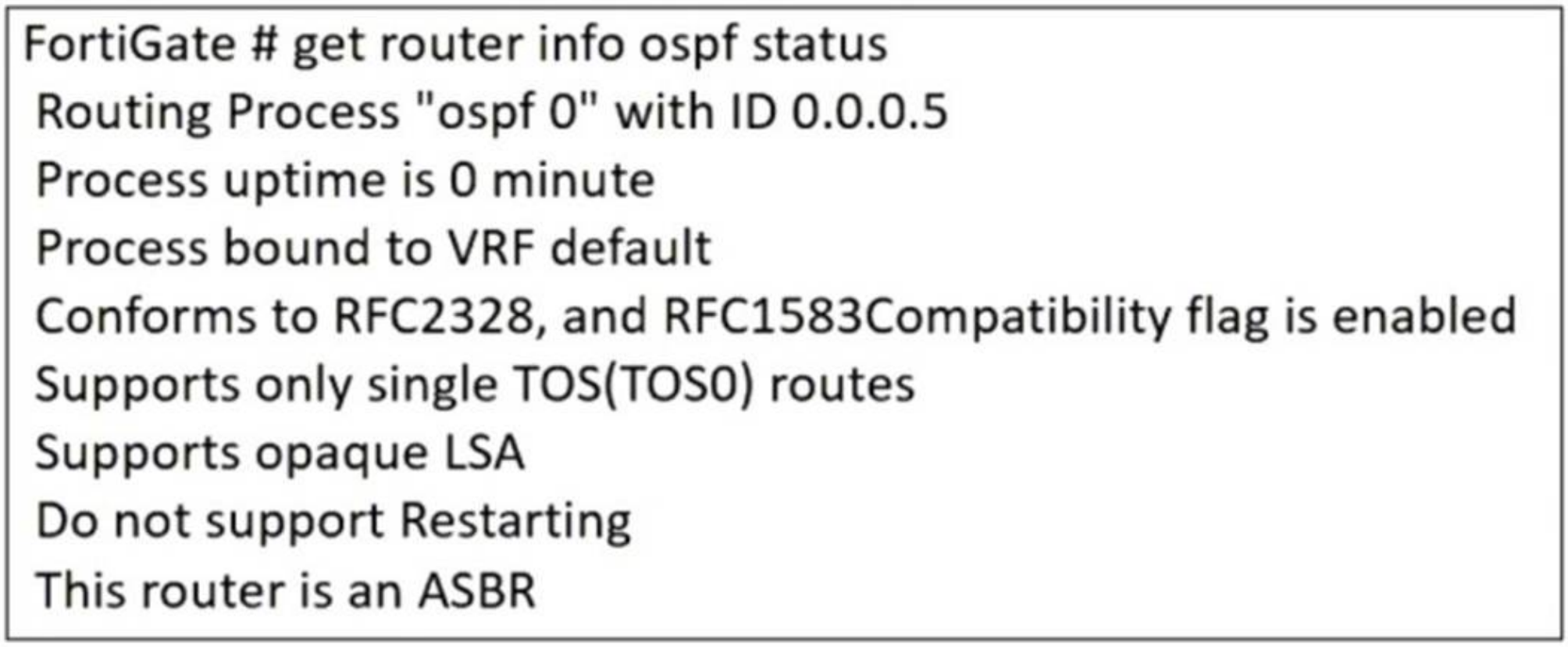
NEW QUESTION 10
An administrator must standardize the deployment of FortiGate devices across branches with consistent interface roles and policy packages using FortiManager.
What is the recommended best practice for interface assignment in this scenario?

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 13
Refer to the exhibit, which contains the partial output of an OSPF command.



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?

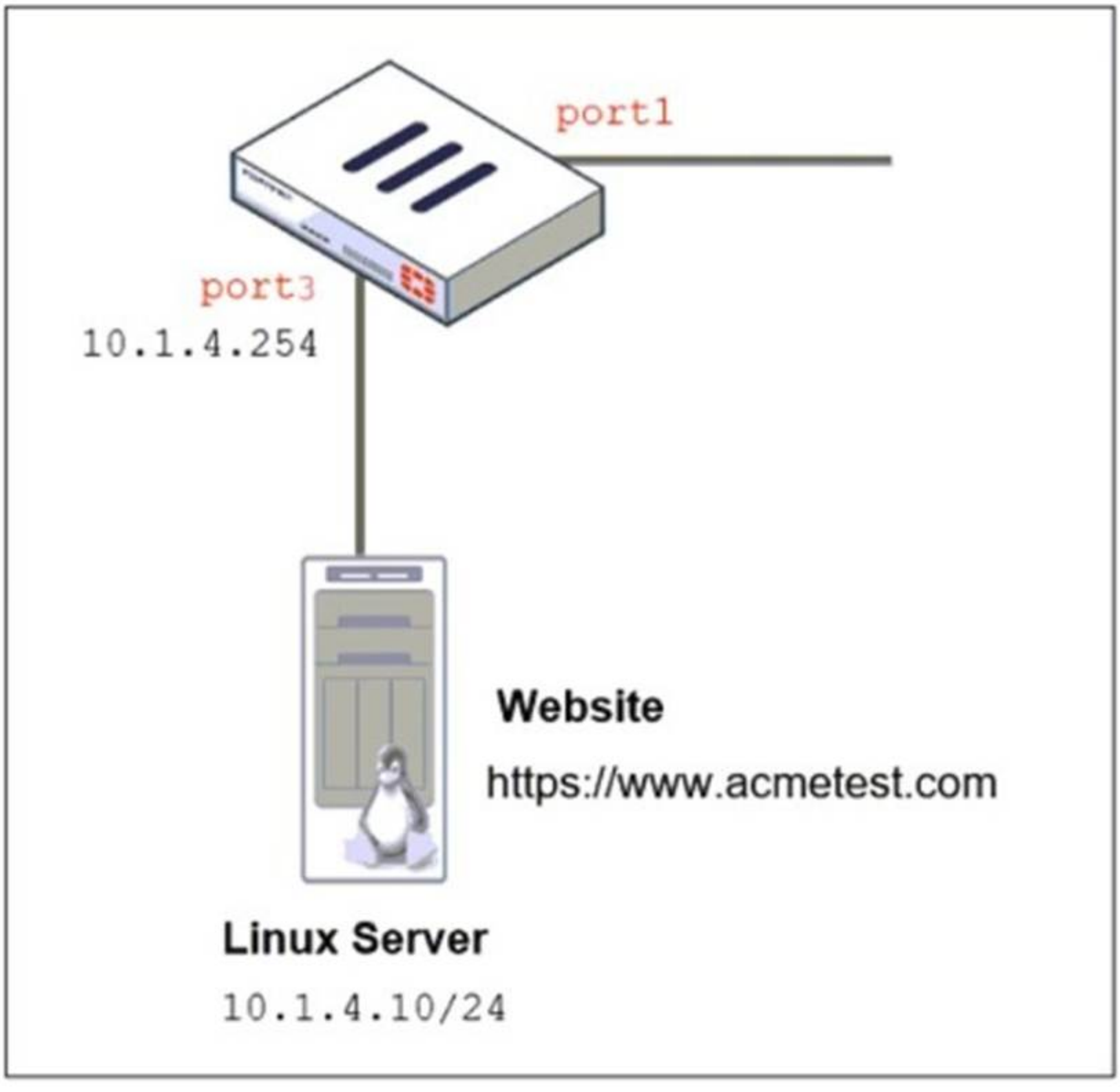
A. The FortiGate device can inject external routing information.
B. The FortiGate device is in the area 0.0.0.5.
C. The FortiGate device does not support OSPF ECMP.
D. The FortiGate device is a backup designated router.

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 15
Refer to the exhibits. The exhibits show a network topology, a firewall policy, and an SSL/SSH inspection profile configuration.

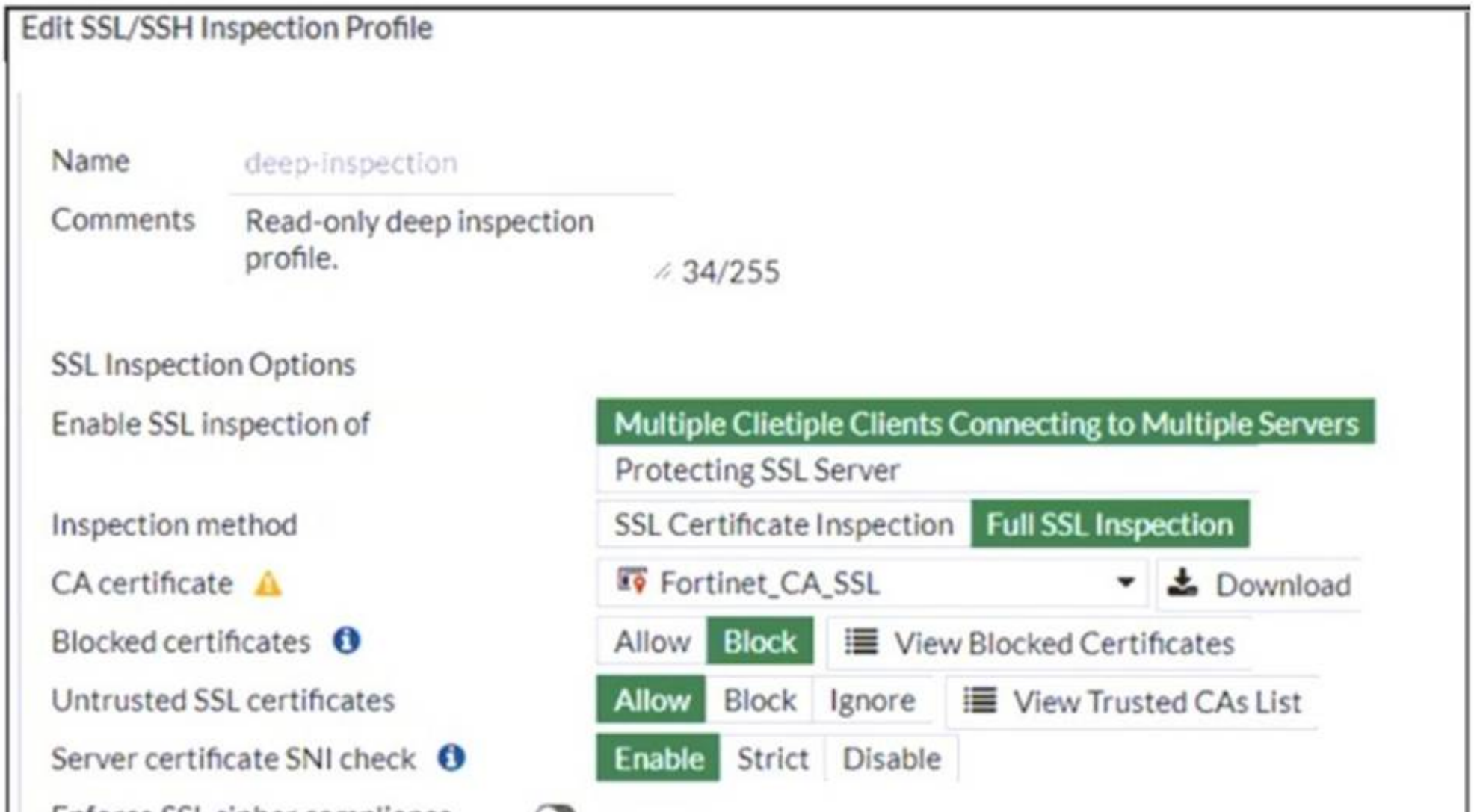
Network Topology



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.

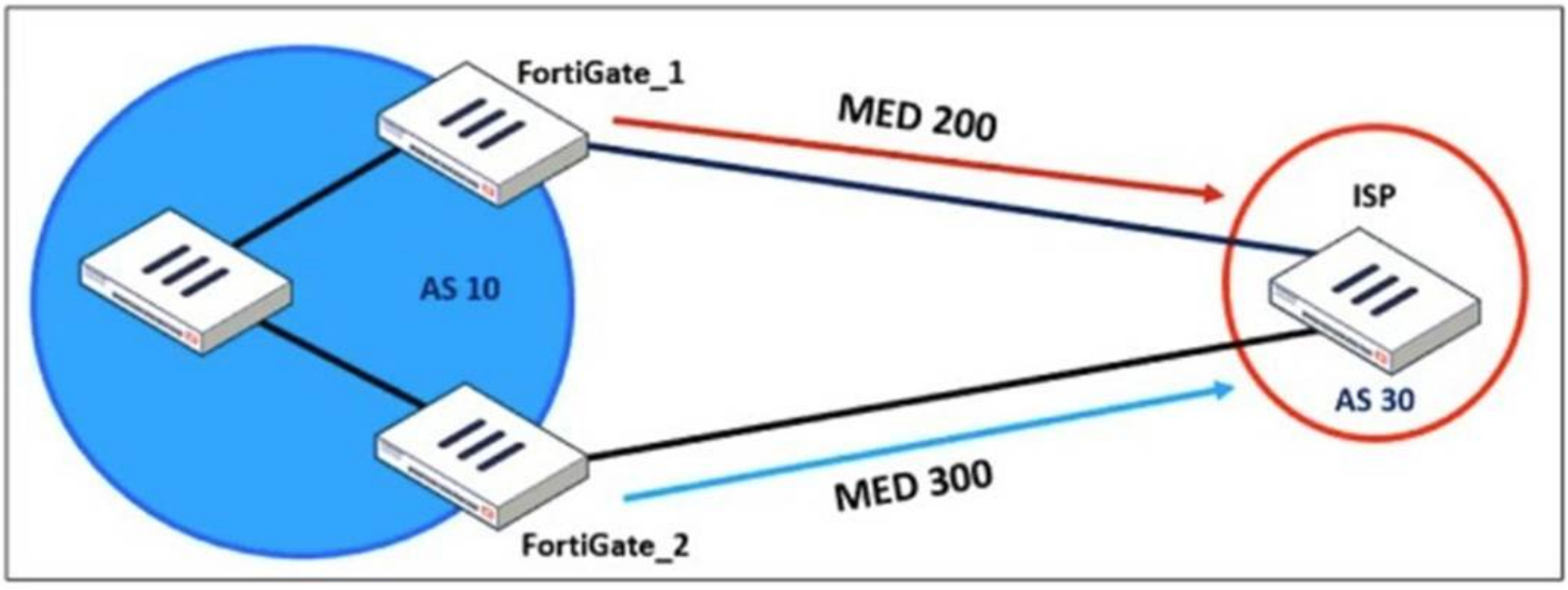
NEW QUESTION 19
A user reports that their computer was infected with malware after accessing a secured HTTPS website. However, when the administrator checks the FortiGate logs, they do not see that the website was detected as insecure despite having an SSL certificate and correct profiles applied on 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 21
Refer to the exhibit, which shows a network diagram.



An administrator would like to modify the MED value advertised from FortiGate_1 to a BGP neighbor in the autonomous system 30.
What must the administrator configure on FortiGate_1 to implement this?

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

Answer: A

Explanation:
TheMulti-Exit Discriminator (MED)is aBGP attributeused to influence the preferred path for incoming traffic from an external autonomous system (AS). The diagram shows that FortiGate_1 advertisesMED 200, while FortiGate_2 advertisesMED 300, meaningthe ISP will prefer the route through FortiGate_1because alower MED is preferredin BGP.
To modify theMED valueon FortiGate_1 for routes advertised to AS 30, the administrator must configure aroute-map-out. A route map canmatch specific routesandset the MED valuebefore sending them to the BGP neighbor.

NEW QUESTION 24
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 26
During the maintenance window, an administrator must sniff all the traffic going through a specific firewall policy, which is handled by NP6 interfaces. The output of the sniffer trace provides just a few packets.
Why is the output of sniffer trace limited?

A. The traffic corresponding to the firewall policy is encrypted.
B. auto-asic-off load is set to enable in the firewall policy,
C. inspection-mode is set to proxy in the firewall policy.
D. The option npudbg is not added in the diagnose sniff packet command.

Answer: B

Explanation:
FortiGate devices withNP6 (Network Processor 6) accelerationoffload traffic directly to hardware, bypassing the CPU for improved performance. Whenauto-asic-offloadis enabled in a firewall policy, most of the trafficdoes not reach the CPU, which means it won't be captured by the standard sniffer trace command.
Since NP6-accelerated traffic is handled entirely in hardware, onlya small portion of initial packets(such as session setup packets or exceptions) might be seen in the sniffer output. To capture all packets, the administrator must disable hardware offloading using:
config firewall policy edit <policy_ID>
set auto-asic-offload disable end
Disabling ASIC offload forces traffic to be processed by the CPU, allowing the sniffer tool to capture all packets.

NEW QUESTION 31
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCSS_EFW_AD-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCSS_EFW_AD-7.4-dumps.html