DUMPSBOSS.

Fortinet NSE 7 - Enterprise Firewall 7.0

Fortinet NSE7_EFW-7.0

Version Demo

Total Demo Questions: 18

Total Premium Questions: 184

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, System Configuration	7
Topic 2, Firewall Policies and Authentication	13
Topic 3, Routing	46
Topic 4, VPN	22
Topic 5, Content Inspection	23
Topic 6, High Availability	13
Topic 7, Central Management	23
Topic 8, Diagnostics and Troubleshooting	37
Total	184

QUESTION NO: 1

An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients send the SYN packets, and before the arrival of the SYN/ACKs. When the SYN/ACK packets arrive to the FortiGate, the unit has already deleted the respective sessions. Which TCP session timer must be increased to fix this problem?

A. TCP half open.

B. TCP half close.

C. TCP time wait.

D. TCP session time to live.

ANSWER: A

Explanation:

TCP half open. is the timer that must be increased. A TCP connection begins with the three-way handshake: the client sends a SYN, the server responds with SYN/ACK, and the client completes the handshake with an ACK. Until FortiGate receives the SYN/ACK response, the session is in a half-open state. The `tcp-halfopen-timer` determines how long FortiGate retains this incomplete TCP session after seeing the initial SYN. In this case, reducing that timer caused FortiGate to age out the session before the server's SYN/ACK arrived. Therefore, when the delayed SYN/ACK reaches FortiGate, there is no matching session state remaining. Increasing the TCP half-open timer allows sufficient time for the SYN/ACK to return and the handshake to complete, while preserving normal stateful inspection. The appropriate value should account for the application's network latency and any intermediate devices or paths that can delay connection establishment. Fortinet documents this setting as the timeout for sessions that have received a SYN but have not yet received a SYN/ACK. See the FortiGate CLI reference for session TTL settings and the FortiGate Administration Guide session TTL documentation.

QUESTION NO: 2

View the exhibit, which contains a partial routing table, and then answer the question below.

Assuming all the appropriate firewall policies are configured, which of the following pings will FortiGate route? (Choose two.)

A. Source IP address 10.1.0.24, Destination IP address 10.72.3.20.

B. Source IP address 10.72.3.27, Destination IP address 10.1.0.52.

C. Source IP address 10.72.3.52, Destination IP address 10.1.0.254.

D. Source IP address 10.73.9.10, Destination IP address 10.72.3.15.

ANSWER: B C

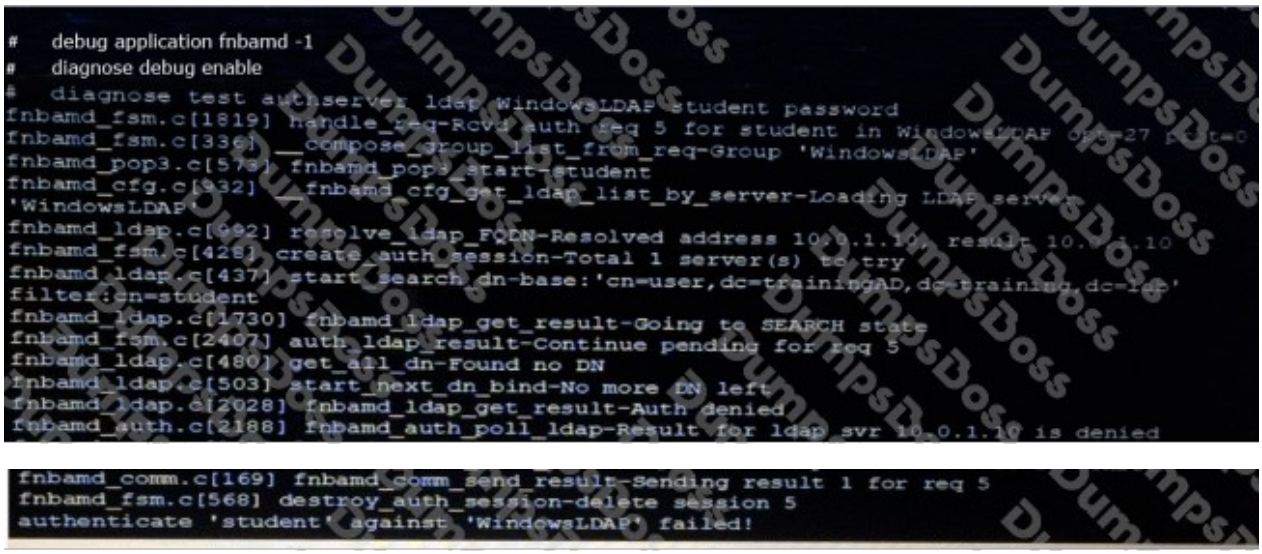
Explanation:

FortiGate can route traffic with source IP address 10.72.3.27 and destination IP address 10.1.0.52, and traffic with source IP address 10.72.3.52 and destination IP address 10.1.0.254. In both cases, the source is within the 10.72.3.0/24 network shown in the routing information and the destination belongs to the reachable 10.1.0.0/24 network. Therefore, after the packet is accepted on the appropriate ingress interface and matches a firewall policy, FortiGate has a valid forwarding path for its destination.

Route selection is based primarily on the destination address. FortiGate evaluates the routing table and selects the most specific matching route, then forwards the packet through the interface and next hop associated with that route. Both 10.1.0.52 and 10.1.0.254 fall within the same matching 10.1.0.0/24 prefix, so they use that route. The different host addresses in 10.72.3.0/24 do not change this destination-route decision. This behavior is consistent with FortiOS routing operation and its longest-prefix-match route lookup process. See the Fortinet Routing administration guide and the FortiGate routing table documentation.

QUESTION NO: 3

An LDAP user cannot authenticate against a FortiGate device. Examine the real time debug output shown in the exhibit when the user attempted the authentication; then answer the question below.



Based on the output in the exhibit, what can cause this authentication problem?

A. User student is not found in the LDAP server.

B. User student is using a wrong password.

C. The FortiGate has been configured with the wrong password for the LDAP administrator.

D. The FortiGate has been configured with the wrong authentication schema.

ANSWER: A

Explanation:

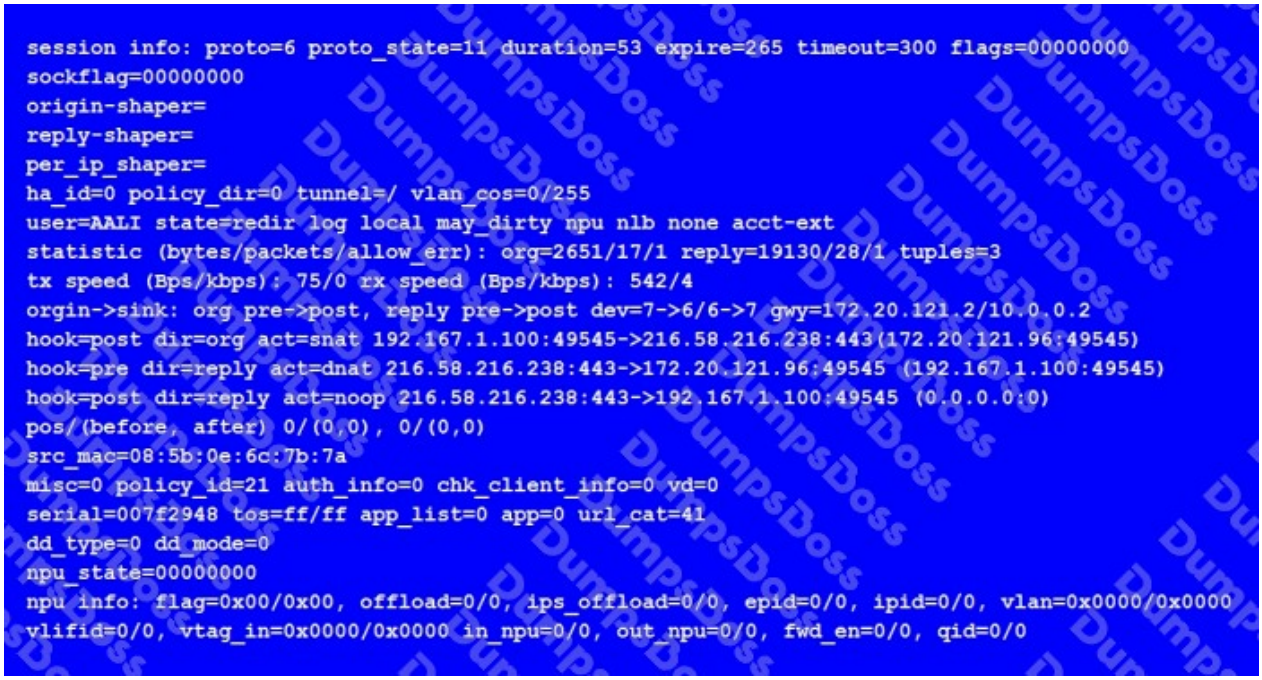
User student is not found in the LDAP server. The debug output indicates that FortiGate can contact the LDAP server and perform the configured LDAP query, but the lookup for the supplied user does not return a matching directory object. This is a user-search failure: FortiGate cannot locate an LDAP entry for `student` within the configured search base and

according to the configured user-name attribute. Consequently, FortiGate has no user distinguished name against which it can perform the user authentication step.

FortiGate LDAP authentication first uses the configured LDAP server details and bind credentials, when applicable, to search the directory for the user. The search base, common-name identifier, and any filter must match the directory structure and attributes containing the account. Confirm that the account exists, that its username is represented by the configured identifier attribute, and that the account resides below the configured distinguished-name search base. Fortinet's LDAP server configuration guidance describes these user lookup fields and their role in directory authentication: FortiGate Administration Guide: LDAP servers. For troubleshooting, Fortinet also documents use of authentication debugging to identify the LDAP lookup stage and returned directory result: Fortinet Community: Debug LDAP authentication issues.

QUESTION NO: 4

View the exhibit, which contains an entry in the session table, and then answer the question below.



Which one of the following statements is true regarding FortiGate's inspection of this session?

A. FortiGate applied proxy-based inspection.

B. FortiGate forwarded this session without any inspection.

C. FortiGate applied flow-based inspection.

D. FortiGate applied explicit proxy-based inspection.

ANSWER: A

Explanation:

FortiGate applied proxy-based inspection. The session-table entry identifies that this traffic was redirected to the antivirus/proxy processing path, rather than remaining solely on the normal flow-processing path. This redirection is characteristic of proxy-based inspection: FortiGate acts as an intermediary for the traffic, receiving and processing content through its proxy engine before forwarding it. Proxy-based inspection supports full protocol-aware content handling and is used when the configured security profile and policy require that inspection architecture.

Session diagnostics are useful for validating the effective processing path of live traffic, particularly when determining whether security inspection prevents hardware offloading or causes a session to be redirected to a content-inspection daemon. Fortinet documents how session-table fields and offload/redirect indicators can be used to identify the handling applied to a session. See Fortinet's session-table inspection guidance and the FortiGate Administration Guide section on inspection modes.

QUESTION NO: 5

An administrator has been assigned the task of creating a set of firewall policies which must be evaluated before any custom policies defined within the policy packages of managed FortiGate devices, across all 25 ADOMSs in FortiManager.

How should the administrator accomplish this task?

A. Create a footer policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this footer policy to all other ADOMs.

B. Create a header policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this header policy to all other ADOMs.

C. Move the FortiGate devices into a single globally scoped ADOM, and merge policy packages, inserting the new firewall policies at the top.

D. Use a CLI script from the root ADOM on FortiManager to push these new policies to all FortiGate devices, through the FGFM tunnel.

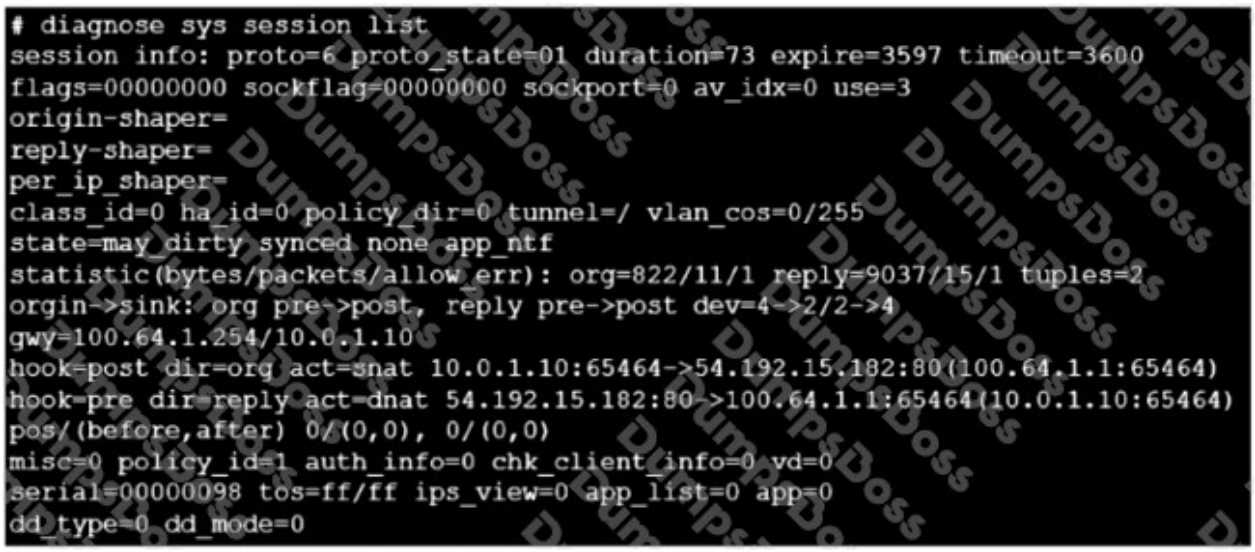
ANSWER: B

Explanation:

Create a header policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this header policy to all other ADOMs. FortiManager's Global ADOM is designed to centrally define policy content that can be assigned to multiple ADOMs, avoiding the need to duplicate the same rules in every local policy package. Global policy packages support header and footer policy sections. When a global header policy is assigned to an ADOM, FortiManager places its rules before the ADOM's local/custom policy rules in the resulting policy package. Because FortiGate evaluates firewall policies in top-down order until a match is found, this placement ensures that the centrally required rules are considered before any custom policies maintained within each managed ADOM. The administrator can therefore create the common rules once in the Global ADOM, use a header policy package, and assign it across all 25 ADOMs. This preserves local ADOM policy administration while enforcing the required global rule precedence consistently. Fortinet documents global policy packages and the header/footer positioning model in the FortiManager Administration Guide and in the NSE 7 Enterprise Firewall study material. See the FortiManager 7.0 Administration Guide and the Fortinet NSE 7 training overview.

QUESTION NO: 6

Refer to the exhibit, which shows the output of diagnose sys session list.



If the HA ID for the primary device is 0, what will happen if the primary fails and the secondary becomes the primary?

A. Traffic for this session continues to be permitted on the new primary device after failover, without requiring the client to restart the session with the server.

B. The secondary device has this session synchronized; however, because application control is applied, the session will be marked dirty and have to be re-evaluated after failover.

C. The session state will be preserved but the kernel will need to re-evaluate the session due to NAT being applied.

D. The session will be removed from the session table of the secondary device due to the presence of allowed error packets, which will force the client to restart the session with the server.

ANSWER: A

Explanation:

Traffic for this session continues to be permitted on the new primary device after failover, without requiring the client to restart the session with the server. The `ha_id=0` value associates the session with the cluster member whose HA ID is 0, which in this case is the original primary. When FGCP HA session synchronization (session pickup) is operating, the primary replicates eligible session-table entries to the secondary. The synchronized entry contains the forwarding state required for the replacement primary to recognize the existing flow after the role change, including protocol state and relevant session handling information such as NAT state when applicable. Consequently, when the secondary is promoted, it can continue processing packets that belong to the already-established client-server connection rather than treating them as a new connection. This is the purpose of session pickup: to reduce or avoid interruption of established traffic during an HA failover. Fortinet describes using `diagnose sys session list` and the HA session information to verify synchronized sessions in its technical note on checking HA session synchronization. Additional HA and session-pickup configuration context is available in the FortiGate 7.0 Administration Guide.

QUESTION NO: 7

Which two statements about FortiManager workspace mode are true? (Choose two.)

A. An administrator must lock an ADOM before making policy and object changes.

B. Changes must be committed before they are available for installation.

C. Enabling workspace mode automatically installs committed changes on managed devices.

D. Workspace mode prevents administrators from creating revision histories.

ANSWER: A B

Explanation:

When workspace mode is enabled, an administrator must lock the ADOM before making changes to policy packages and objects in that ADOM. The lock prevents concurrent administrators from making conflicting database changes while one administrator is editing the workspace.

Workspace mode also requires the administrator to commit changes to save them to the FortiManager database. Until the changes are committed, they remain in the administrator's private workspace and are not available for installation to managed FortiGate devices. The commit operation is separate from installing the resulting configuration to devices. See the FortiManager 7.0 Administration Guide.

QUESTION NO: 8

How are bulk configuration changes made using FortiManager CLI scripts? (Choose two.)

A. When run on the All FortiGate in ADOM, changes are automatically installed without the creation of a new revision history.

B. When run on the Device Database, changes are applied directly to the managed FortiGate device.

C. When run on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

D. When run on the Policy Package, ADOM database, you must use the installation wizard to apply the changes to the managed FortiGate device

ANSWER: C D

Explanation:

Running a CLI script on the Remote FortiGate directly sends the commands immediately to the selected managed FortiGate or FortiGates through the remote CLI connection. Because this execution method bypasses the normal FortiManager database-to-install workflow, FortiManager does not provide a pre-install preview or validation step for the resulting device configuration changes. This method is appropriate when an administrator intentionally needs to execute commands directly, while accepting that the changes are applied without the usual installation review process.

Running a CLI script on the Policy Package, ADOM database applies policy- and ADOM-level changes to FortiManager's configuration database first. The changes therefore remain staged in FortiManager until they are deployed. Administrators use the installation wizard to install the updated policy package and associated ADOM database changes on the managed FortiGate devices. This workflow supports reviewing the pending installation scope and deploying the approved configuration consistently across the selected targets. Fortinet documents these CLI-script execution targets and the associated installation workflow in the FortiManager 7.0 Administration Guide and the FortiManager 7.0 CLI Reference.

QUESTION NO: 9

Which of the following conditions must be met for a static route to be active in the routing table? (Choose three.)

A. The next-hop IP address is up.

B. There is no other route, to the same destination, with a higher distance.

C. The link health monitor (if configured) is up.

D. The next-hop IP address belongs to one of the outgoing interface subnets.

E. The outgoing interface is up.

ANSWER: C D E

Explanation:

A static route is eligible to become active only when FortiGate can use its configured egress path and validate the gateway relationship. "The outgoing interface is up." is required because an administratively or operationally unavailable interface cannot forward traffic. "The next-hop IP address belongs to one of the outgoing interface subnets." ensures that the configured gateway is directly reachable through that interface, allowing FortiGate to resolve the next hop at Layer 2 and install a usable route. This is the normal requirement for an interface-and-gateway static route.

"The link health monitor (if configured) is up." is also required when the static route is associated with link-monitor/Dead Gateway Detection behavior. A failed health check marks the monitored path unavailable, so FortiGate withdraws or deactivates the route to prevent forwarding traffic over a failed WAN path. When monitoring subsequently succeeds, the route can again be considered active, provided the interface and gateway requirements remain satisfied. Fortinet documents that static routes depend on interface status and that link monitoring can control route availability for failed links. See the FortiGate static routes documentation and the FortiGate link monitor documentation.

QUESTION NO: 10

Which two statements about FSSO user detection methods are true? (Choose two.)

A. DC Agent mode collects logon information from domain controller security event logs.

B. Workstation polling can query user-session information through remote registry access.

C. FortiGate polls Active Directory workstations directly when workstation polling is enabled.

D. DC Agent mode requires the Remote Registry service to be running on every user workstation.

ANSWER: A B

Explanation:

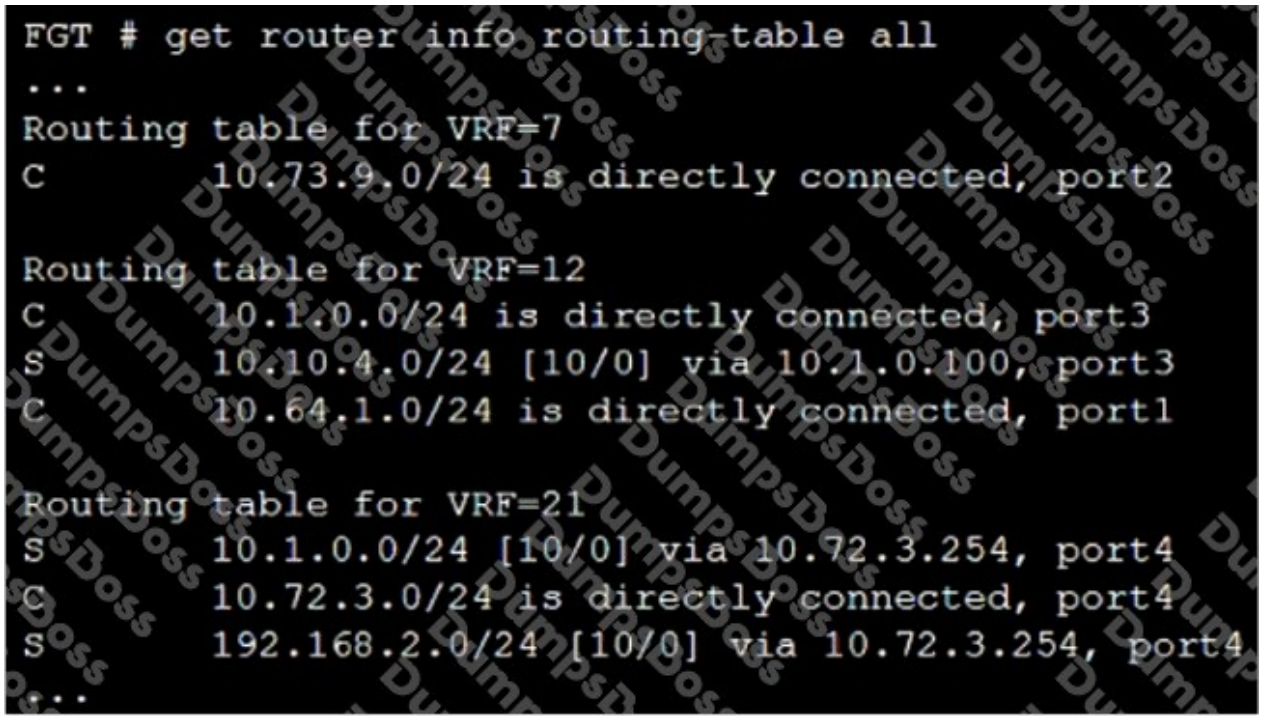
The Collector Agent can use DC Agent mode to obtain logon information from domain controllers. The DC Agent monitors Windows security event logs and forwards detected user logon events to the Collector Agent.

Workstation polling is another FSSO detection method. In this mode, the Collector Agent queries workstations for user-session information, commonly through remote registry access. Therefore, the Remote Registry service and related network access must be available on polled workstations.

Fortinet documents FSSO methods and Collector Agent operation in the FortiGate FSSO documentation.

QUESTION NO: 11

Refer to the exhibit, which shows a partial routing table.



Assuming all the appropriate firewall policies are configured, what two changes would an administrator need to make if they wanted to send traffic from a client directly connected to port3, to a server directly connected to port4? (Choose two.)

A. Configure route leaking between VRF 12 and VRF 21.

B. Disable auto-asic-offload as this is not supported between VRF instances.

C. Configure RIPv2 to exchange route information between the VRF instances.

D. Configure route leaking between port3 and port4.

E. Enable SNAT on the relevant firewall policies to prevent RPF check drops.

ANSWER: A B

Explanation:

Traffic crossing from an interface assigned to VRF 12 to an interface assigned to VRF 21 requires explicit route leaking between the two VRF routing tables. VRFs maintain separate routing domains, so a route in one VRF is not automatically

available to another. The administrator must configure routes that leak the client and server network prefixes as needed, including return-path reachability, so that each VRF can resolve the destination through the appropriate egress interface.

The firewall policy that carries inter-VRF traffic must also have ASIC offloading disabled. FortiGate hardware acceleration does not support forwarding sessions between VRF instances in this scenario. Disabling automatic ASIC offloading ensures that the traffic is processed by the CPU-based forwarding path, where the VRF lookup and route-leaking behavior are applied correctly. This is configured on the relevant firewall policy using the `auto-asic-offload` setting.

Fortinet documents VRF configuration and the separation of routing tables in the FortiOS 7.0 Administration Guide. The associated policy configuration commands, including ASIC-offload controls, are available in the FortiOS 7.0 CLI Reference.

QUESTION NO: 12

Refer to the exhibit, which contains partial output from an IKE real-time debug.

Which two statements about this debug output are correct? (Choose two.)

A. The remote gateway IP address is 10.0.0.1.

B. The initiator provided remote as its IPsec peer ID.

C. It shows a phase 1 negotiation.

D. The negotiation is using AES128 encryption with CBC hash.

ANSWER: B C

Explanation:

The statement **"The initiator provided remote as its IPsec peer ID."** is correct because the IKE debug identifies the peer ID received from the initiating endpoint as `remote`. During IKE authentication, peer identifiers are exchanged and evaluated

against the phase 1 configuration. These identifiers can be an IP address, FQDN, user FQDN, or an explicitly configured string, and they are used to identify the remote IKE peer independently of the packet source address.

The statement **"It shows a phase 1 negotiation."** is also correct. The displayed IKE messages and security-association processing belong to establishment of the IKE SA, commonly called IPsec phase 1. Phase 1 creates the protected and authenticated IKE management channel that is subsequently used to negotiate the IPsec child SA, or phase 2. FortiGate IKE debug output is therefore useful for distinguishing an IKE-SA establishment issue from a later IPsec-SA negotiation issue. Fortinet documents the IKE/IPsec negotiation sequence and troubleshooting workflow in its IPsec VPN administration documentation and IKE debugging guidance.

QUESTION NO: 13

Which two statements about application-layer test commands are true? (Choose two.)

A. Some of them display real-time application debugs.

B. Some of them can be used to restart an application.

C. Some of them display statistics and configuration information about a feature or process.

D. Some of them only display output, after you run the diagnose debug console enable command.

ANSWER: B C

Explanation:

Application-layer test commands are implemented through the FortiOS `diagnose test application` command family. They expose diagnostic operations that are specific to individual daemons and features, with the available subcommands depending on the application being tested. A common use is controlling a daemon or feature process, including initiating a restart where that application provides a restart test operation. This makes *Some of them can be used to restart an application.* correct.

These commands can also return operational information maintained by the relevant process. Depending on the daemon and test selector, the output can include counters, runtime status, internal state, and feature-related configuration or settings. Therefore, *Some of them display statistics and configuration information about a feature or process.* is also correct. Administrators should first use the application test command's help or list function to identify the supported selectors for the specific FortiOS process, because supported operations are not uniform across all applications. Fortinet documents diagnostic CLI commands and application-specific test operations in its FortiOS CLI reference and administration documentation: FortiOS 7.0 CLI Reference and FortiOS 7.0 Administration Guide.

QUESTION NO: 14

An administrator has configured an SD-WAN rule that uses the Best Quality strategy. Two members meet the SLA requirements configured in the health check.

Which member does FortiGate select for a new session?

A. The eligible member with the best SLA performance.

B. The eligible member with the lowest configured cost.

C. The first member listed in the SD-WAN rule.

D. The member with the highest interface bandwidth.

ANSWER: A

Explanation:

FortiGate selects the eligible SD-WAN member with the best measured quality according to the configured SLA criteria. The Best Quality strategy evaluates the health-check performance measurements, such as latency, jitter, and packet loss, and chooses the member that provides the best result among members that satisfy the SLA.

This differs from the Lowest Cost strategy, which selects an eligible member based on configured cost, and the Manual strategy, which follows the configured member order. Existing sessions are normally retained on their selected member unless a condition requires them to be moved. See the FortiGate 7.0 Administration Guide.

QUESTION NO: 15

Which real time debug should an administrator enable to troubleshoot RADIUS authentication problems?

A. Diagnose debug application radius -1.

B. Diagnose debug application fnbamd -1.

C. Diagnose authd console –log enable.

D. Diagnose radius console –log enable.

ANSWER: B

Explanation:

Diagnose debug application fnbamd -1. is the appropriate real-time application debug because `fnbamd` is the FortiGate daemon that handles firewall user authentication and communicates with external authentication servers, including RADIUS servers. Enabling its maximum debug level shows the authentication workflow in real time: the user and group lookup context, the selected RADIUS server, Access-Request processing, received replies such as Access-Accept or Access-Reject, timeout behavior, and authentication-result handling. This information lets an administrator correlate a login attempt with the FortiGate's interaction with the configured RADIUS service and identify where processing fails.

In practice, the administrator should first enable debug output with `diagnose debug enable`, run `diagnose debug application fnbamd -1`, reproduce the authentication attempt, and then disable debugging afterward with `diagnose debug disable`. Debug output can include operationally sensitive details and can be verbose, so it should be enabled only for the time needed to capture the issue. Fortinet documents application-debug operation in the FortiGate CLI reference; Fortinet's troubleshooting guidance also identifies `fnbamd` debugging for authentication investigations in its fnbamd debug technical tip.

QUESTION NO: 16

In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two.)

A. It provides VM license validation services.

B. It supports rating requests from non-FortiGate devices.

C. It caches available firmware updates for unmanaged devices.

D. It can be configured as an update server, a rating server, or both.

ANSWER: A D

Explanation:

When deployed as a local FortiGuard Distribution Server (FDS), FortiManager can provide VM license validation services. This lets FortiManager act as the on-premises validation point for FortiGate-VM licensing, which is particularly useful in restricted or isolated environments where managed virtual firewalls cannot directly reach FortiGuard licensing services on the internet. FortiManager can also be configured as an update server, a rating server, or both. In update-server mode, it obtains and distributes eligible FortiGuard update packages to managed FortiGates. In rating-server mode, it handles FortiGuard query services, such as web-filtering categorization requests. These roles can be enabled independently or

together, allowing the deployment to match local connectivity, security, and service requirements. FortiManager documentation describes its local FDS capability and the available update, rating, and VM-license-validation functions. See the FortiManager 7.0 Administration Guide and Fortinet's FortiManager 7.0 New Features documentation.

QUESTION NO: 17

Refer to the exhibit, which shows the output of a diagnose command.

```
FGT # diagnose debug rating
Locale       : english
Service      : Web-filter
Status       : Enable
License      : Contract
Service      : Antispam
Status       : Disable
Service      : Virus Outbreak Prevention
Status       : Disable
 -=- Server List (Mon Apr 19 10:41:32 20xx) -=-
IP                 Weight  RTT    Flags   TZ  Packets   Curr Lost    Total Lost
64.26.151.37        10     45             -5  262432    0            846
64.26.151.35        10     46             -5  329072    0            6806
66.117.56.37        10     75             -5  71638     0            275
65.210.95.240       20     71             -8  36875     0            92
209.222.147.36      20     103     DI     -8  34784     0            1070
208.91.112.194      20     107     D      -8  35170     0            1533
96.45.33.65         60     144             0  33728     0            120
80.85.69.41         71     226             1  33797     0            192
62.209.40.74        150    97              9  33754     0            145
121.111.236.179     45     44      F      -5  26410     26226        26227
```

What can be concluded about the debug output in this scenario?

A. Servers with a negative TZ value are less preferred for rating requests.

B. There is a natural correlation between the value in the Packets field and the value in the Weight field.

C. FortiGate used 64.26.151.37 as the initial server to validate its contract.

D. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.

ANSWER: B

Explanation:

There is a natural correlation between the value in the Packets field and the value in the Weight field. The `diagnose debug rating` output displays the FortiGuard rating servers known to the FortiGate and includes operational values used in rating-server selection. The Packets value represents the number of rating requests handled by a server, while Weight reflects the relative selection weighting associated with that server. As traffic is sent to a rating server, its packet count and weight are updated as part of the load-distribution process. This lets FortiGate avoid continually selecting one server while other available FortiGuard servers can process requests. Therefore, the displayed progression of packet counters alongside their weights is expected behavior rather than a server preference based on time zone or DNS answer order. This diagnostic view is useful when investigating how web-filter and other FortiGuard rating requests are being distributed among reachable servers. Fortinet documents FortiGuard connectivity, server selection, and diagnostic procedures in the FortiOS 7.0 Administration Guide and its FortiOS 7.0 CLI Reference.

QUESTION NO: 18

An administrator wants to verify whether FortiGate has successfully resolved the MAC address of an IPv4 next-hop gateway on port1.

Which command provides this information?

A. get system arp

B. get router info routing-table all

C. diagnose sys session list

D. diagnose ip address list

ANSWER: A

Explanation:

`get system arp` displays the IPv4 ARP table, including IP-to-MAC address mappings learned by FortiGate. The administrator can use this output to verify that the configured next-hop gateway has an ARP entry associated with the expected interface.

If the next-hop gateway is directly connected and no ARP entry can be resolved, FortiGate cannot send Ethernet frames to that gateway. Reviewing ARP output together with interface status, routing-table entries, and packet captures helps isolate Layer 2 or Layer 3 forwarding problems. See the FortiOS 7.0 CLI Reference.