DUMPSBOSS.

Fortinet EMEA Advanced Support Exam

Fortinet EMEA-Advanced-Support

Version Demo

Total Demo Questions: 7

Total Premium Questions: 72

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which FortiGate feature allows for policy-based routing?

A. SD-WAN Rules

B. Policy Routes

C. Static Routes

D. Dynamic Routes

ANSWER: B

Explanation:

Policy Routes is the FortiGate feature designed for policy-based routing. A policy route defines forwarding behavior using criteria beyond the destination-prefix lookup normally performed against the routing table. Administrators can match traffic by characteristics such as source address, destination address, incoming interface, protocol, and ports, then specify the gateway and outgoing interface to use. This permits selected traffic flows to take a particular path—for example, forwarding a defined source subnet or application service through a designated ISP—regardless of the route that would otherwise be selected by the normal routing-table process. FortiGate evaluates policy routes before the standard route lookup for traffic that matches their configured conditions, so they provide explicit, criteria-driven control of packet forwarding. This capability is particularly useful where routing requirements depend on the identity or type of traffic rather than solely on its destination network. Fortinet documents policy routes as routes that apply matching rules to packets and direct them to a specified next hop or interface. See the FortiGate Administration Guide: Policy routes and the FortiGate Administration Guide: Routing.

QUESTION NO: 2

Users report that an application session is successful through a FortiGate, but no traffic log is available for investigation. Which two conditions are required for successful sessions matching a firewall policy to be recorded as traffic logs? (Select two)

A. The matching firewall policy is configured to log the relevant traffic

B. A configured logging destination is available to receive or store the logs

C. The policy uses source NAT

D. The policy has an IPS profile enabled

E. The route to the destination has an administrative distance of 10

ANSWER: A B

Explanation:

The matching firewall policy must be configured to log the relevant traffic, and FortiGate must have an available logging destination. For full visibility of permitted sessions, the policy can use a traffic logging setting such as logging all sessions. FortiGate must also be able to write the generated logs to a configured destination, such as local disk, FortiAnalyzer, FortiCloud, or another supported logging target.

A route to the destination network is required for the traffic session itself, but it does not enable log generation. Enabling a security profile may create security-event logs when a profile detects something, but it does not replace normal traffic logging for all successful sessions.

QUESTION NO: 3

Which two statements are correct about TCP Maximum Segment Size (MSS) and FortiGate TCP MSS rewriting? (Select two)

A. TCP MSS specifies the maximum TCP payload size and excludes IP and TCP headers

B. FortiGate TCP MSS rewriting changes the MSS value advertised during the TCP handshake

C. TCP MSS includes the complete Ethernet frame size

D. TCP MSS rewriting changes the configured IP MTU of an interface

E. TCP MSS rewriting controls the payload size of UDP datagrams

ANSWER: A B

Explanation:

TCP MSS specifies the maximum TCP payload size and does not include the IP and TCP headers. For a standard IPv4 TCP packet without options, the total packet size is the MSS plus a 20-byte IPv4 header and a 20-byte TCP header.

FortiGate TCP MSS rewriting changes the MSS value advertised during the TCP handshake. This can prevent packets from exceeding the effective path MTU, particularly when encapsulation such as IPsec adds overhead.

TCP MSS does not apply to UDP traffic, and MSS rewriting does not change the IP MTU configured on an interface.

QUESTION NO: 4

A client initiates an outbound connection through a FortiGate policy with source NAT enabled. How does FortiGate handle the returning packets from the external server?

A. FortiGate matches the return traffic to the existing session and reverses the source translation

B. FortiGate requires a separate inbound allow policy for every reply packet

C. FortiGate forwards the reply to the default gateway without checking session state

D. FortiGate creates a new outbound session for the returning traffic

ANSWER: A

Explanation:

FortiGate matches the return traffic to the existing session and reverses the source translation is correct. When source NAT is applied to the outbound session, FortiGate stores the translation and session-state information. Reply traffic arriving from the external server is matched against that session, then the destination is translated back to the original internal client address.

A separate reverse firewall policy is normally not required for valid return traffic because FortiGate is stateful. However, asymmetric routing or traffic that does not return through the FortiGate can prevent the existing session from being matched correctly.

QUESTION NO: 5

Which two traffic flows are candidates for control by a FortiGate local-in policy? (Select two)

A. An administrator opening HTTPS to the FortiGate WAN interface address

B. An IPsec peer sending IKE traffic to the FortiGate WAN address

C. A LAN client browsing an Internet web server through FortiGate

D. A remote VPN user connecting to an internal file server

E. A LAN client accessing a server published through a Virtual IP

ANSWER: A B

Explanation:

A local-in policy controls traffic destined to the FortiGate itself rather than traffic transiting through the firewall. HTTPS administrative access to an interface address is destined to the FortiGate management plane. IKE negotiation traffic sent to a FortiGate WAN address is also destined to the FortiGate because the device must process it to establish an IPsec VPN.

Traffic from a LAN client to an Internet server, or from a VPN user to an internal server, transits the FortiGate and is controlled by regular firewall policies. A local-in policy does not replace the firewall policies required for those forwarded sessions.

QUESTION NO: 6

Hybrid cloud means that

A. The cloud provider uses AMD, Intel and possibly also other CPU vendors

B. Some of the customer's systems are virtualized in the public cloud and some are in the local datacenter

C. One customer uses VMs with multiple different operating systems in the same cloud account

D. Cloud provider provides both 32-bit and 64-bit virtual machines

ANSWER: B

Explanation:

Some of the customer's systems are virtualized in the public cloud and some are in the local datacenter is correct because a hybrid cloud connects and uses both on-premises infrastructure and public-cloud services as parts of the same overall computing environment. An organization can retain selected applications, data, or services in its local datacenter while placing other workloads in a public cloud. This model supports operational flexibility, gradual migration, and placement of workloads according to technical, security, compliance, latency, and capacity requirements. The defining characteristic is therefore the combination of local and public-cloud environments, not a particular processor, operating-system mix, or virtual-machine architecture. Fortinet supports securing these distributed environments through cloud-delivered and virtualized security controls, including FortiGate-VM deployments and centralized security management across cloud and on-premises locations. Fortinet describes its public-cloud security offerings and integrations at Fortinet Public Cloud Security. For a general description of hybrid-cloud architecture and its use of on-premises and cloud resources, see AWS Hybrid Cloud.

QUESTION NO: 7

What is the purpose of the FortiGate â€˜diagnose debug flowâ€™ command?

A. To display real-time packet captures

B. To troubleshoot routing table issues

C. To show the packet flow through firewall policies

D. To monitor system performance metrics

ANSWER: C

Explanation:

The purpose of `diagnose debug flow` is to show how FortiGate processes a packet as it traverses the firewall's traffic-handling path. After enabling debug flow and starting a trace, an administrator can inspect the decision points that affect the session, such as the incoming interface, route lookup, firewall-policy lookup, policy ID selected, source or destination NAT processing, session creation, and the reason a packet is accepted or denied. This is especially valuable when traffic does

not pass as expected even though the configuration appears correct, because the trace identifies the actual policy and processing outcome applied to the packet. Administrators normally narrow the output with flow filters, such as a source address, destination address, protocol, or port, before collecting a limited number of trace packets. Fortinet documents debug flow as a tool for diagnosing traffic by tracing packet processing through the FortiGate system. See the FortiGate Administration Guide: Diagnosing traffic with debug flow and the Fortinet Community technical tip on diagnose debug flow.