# Fortinet
# FCP_FGT_AD-7.4
## FCP - FortiGate 7.4 Administrator

**Questions And Answers PDF Format:**

**For More Information – Visit link below:**
**https://www.certsgrade.com/**

*Version* = **Product**

# Latest Version: 7.0

## Question: 1

Refer to the exhibit.

**FortiGate routing database**

```
Local-FortiGate # get router info routing-table database
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
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 10.200.2.254, port2, [1/0]
S    *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C    *> 10.0.1.0/24 is directly connected, port3
C    *> 10.200.1.0/24 is directly connected, port1
C    *> 10.200.2.0/24 is directly connected, port2
C    *> 172.16.100.0/24 is directly connected, port8
```

Which two statements are true about the routing entries in this database table? (Choose two.)

A. All of the entries in the routing database table are installed in the FortiGate routing table.
B. The port2 interface is marked as inactive.
C. Both default routes have different administrative distances.
D. The default route on porc2 is marked as the standby route.

**Answer: C, D**

Explanation:
The routing table in the exhibit shows two default routes (0.0.0.0/0) with different administrative distances:
The default route through port2 has an administrative distance of 20.
The default route through port1 has an administrative distance of 10.
Administrative distance determines the priority of the route; a lower value is preferred. Here, the route through port1 with an administrative distance of 10 is the preferred route. The route through port2 with an administrative distance of 20 acts as a standby or backup route. If the primary route (port1) fails or is unavailable, traffic will then be routed through port2.
Regarding the statement that the port2 interface is marked as inactive, there is no indication in the

routing table that port2 is inactive. Similarly, all the routes displayed are not necessarily installed in the FortiGate routing table, as the table could include both active and backup routes.
Reference:
FortiOS 7.4.1 Administration Guide: Default route configuration
FortiOS 7.4.1 Administration Guide: Routing table explanation

## Question: 2

Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

A. The host field in the HTTP header.
B. The server name indication (SNI) extension in the client hello message.
C. The subject alternative name (SAN) field in the server certificate.
D. The subject field in the server certificate.
E. The serial number in the server certificate.

**Answer: B, C, D**

Explanation:
When SSL certificate inspection is enabled on a FortiGate device, the system uses the following three pieces of information to identify the hostname of the SSL server:
Server Name Indication (SNI) extension in the client hello message (B): The SNI is an extension in the client hello message of the SSL/TLS protocol. It indicates the hostname the client is attempting to connect to. This allows FortiGate to identify the server's hostname during the SSL handshake.
Subject Alternative Name (SAN) field in the server certificate (C): The SAN field in the server certificate lists additional hostnames or IP addresses that the certificate is valid for. FortiGate inspects this field to confirm the identity of the server.
Subject field in the server certificate (D): The Subject field contains the primary hostname or domain name for which the certificate was issued. FortiGate uses this information to match and validate the server's identity during SSL certificate inspection.
The other options are not used in SSL certificate inspection for hostname identification:
Host field in the HTTP header (A): This is part of the HTTP request, not the SSL handshake, and is not used for SSL certificate inspection.
Serial number in the server certificate (E): The serial number is used for certificate management and revocation, not for hostname identification.
Reference
FortiOS 7.4.1 Administration Guide - SSL/SSH Inspection, page 1802.
FortiOS 7.4.1 Administration Guide - Configuring SSL/SSH Inspection Profile, page 1799.

## Question: 3

Refer to the exhibit.

| ID | Name | Source | Destination | Criteria | Members |
|---|---|---|---|---|---|
| IPv4 3 | | | | | |
| 1 | Critical-DIA | LOCAL_SUBNET | Slack-Slack<br>Dropbox-Web<br>Bloomberg | | port1<br>port2 |
| 2 | Non-Critical-DIA | LOCAL_SUBNET | Addicting.Games<br>Social.Media | Bandwidth | port2 |
| 3 | Default-Internet | LOCAL_SUBNET | REMOTE_SUBNET | Latency | port1<br>port2 |
| Implicit 1 | | | | | |
| | sd-wan | all | all | Source-Destination IP | any |

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

A. All traffic from a source IP to a destination IP is sent to the same interface.
B. Traffic is sent to the link with the lowest latency.
C. Traffic is distributed based on the number of sessions through each interface.
D. All traffic from a source IP is sent to the same interface

**Answer: A**

Explanation:
For traffic that does not match any of the defined SD-WAN rules, the default implicit SD-WAN rule is applied. By default, the FortiGate uses a "source-destination IP-based" algorithm, which means all traffic from a specific source IP to a specific destination IP is sent through the same interface. This ensures that a consistent path is used for traffic between the same source and destination IP addresses. Options B, C, and D do not apply because the default algorithm does not prioritize by latency, session count, or source IP alone.
Reference:
FortiOS 7.4.1 Administration Guide: SD-WAN Load Balancing Algorithms

## Question: 4

A network administrator is configuring an IPsec VPN tunnel for a sales employee travelling abroad.
Which IPsec Wizard template must the administrator apply?

A. Remote Access
B. Site to Site
C. Dial up User
D. iHub-and-Spoke

**Answer: A**

Explanation:
For configuring an IPsec VPN tunnel for a sales employee traveling abroad, the "Remote Access" template is the most appropriate choice. This template is designed to allow remote users to securely

connect to the internal network of an organization from any location using FortiClient or a compatible client. The other options, such as "Site to Site," "Dial up User," and "iHub-and-Spoke," are used for connecting different networks or sites, not individual remote users.
Reference:
FortiOS 7.4.1 Administration Guide: IPsec Wizard Template Types

## Question: 5

Refer to the exhibits, which show the system performance output and the default configuration of high memory usage thresholds in a FortiGate.

System Performance output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Based on the system performance output, what can be the two possible outcomes? (Choose two.)

A. FortiGate will start sending all files to FortiSandbox for inspection.
B. FortiGate has entered conserve mode.
C. Administrators cannot change the configuration.
D. Administrators can access FortiGate onlythrough the console port.

**Answer: B, D**

Explanation:

Based on the system performance output provided, the memory usage on the FortiGate device is at 90%, which is above the green threshold (82%) but below the red threshold (88%). Given this high memory usage, the FortiGate device will enter "conserve mode" to prevent further resource exhaustion.
In conserve mode:
B . FortiGate has entered conserve mode: When the memory usage reaches or exceeds certain thresholds (in this case, the green and red thresholds), the FortiGate enters conserve mode to protect itself from running out of memory entirely. This mode limits some functionalities to reduce memory usage and avoid a potential system crash.
D . Administrators can access FortiGate only through the console port: During conserve mode, administrative access might be restricted, and administrators may only be able to connect to the device via the console port. This restriction is in place to ensure that the FortiGate can be managed directly, even under low resource conditions.
The other options are not correct:
A . FortiGate will start sending all files to FortiSandbox for inspection: This is unrelated to memory usage and conserve mode.
C . Administrators cannot change the configuration: While access may be limited, configuration changes can still be made via the console port.
Reference
FortiOS 7.4.1 Administration Guide - Monitoring System Resources and Performance, page 325.
FortiOS 7.4.1 Administration Guide - Conserve Mode, page 330.

For More Information – Visit link below:
https://www.certsgrade.com/

# PRODUCT FEATURES

- 100% Money Back Guarantee
- 90 Days Free updates
- Special Discounts on Bulk Orders
- Guaranteed Success
- 50,000 Satisfied Customers
- 100% Secure Shopping
- Privacy Policy
- Refund Policy

**16 USD Discount Coupon Code: NB4XKTMZ**