



QUESTION & ANSWER

HIGHER QUALITY, BETTER SERVICE

Provide One Year Free Update!

<https://www.passquestion.com>

Exam : **NSE4_FGT_AD-7.6**

Title : Fortinet NSE 4 - FortiOS 7.6
Administrator

Version : DEMO

1.Refer to the exhibit.

FortiGate SD-WAN zone configuration



An SD-WAN zone configuration on the FortiGate GUI is shown. Based on the exhibit, which statement is true?

- A. The Underlay zone contains no member.
- B. The virtual-wan-link and overlay zones can be deleted
- C. The Underlay zone is the zone by default.
- D. port2 and port3 are not assigned to a zone.

Answer: A

Explanation:

According to the FortiOS 7.6 Administrator Guide and the specific behavior of the SD-WAN GUI, here is the technical breakdown:

SD-WAN Zone Hierarchy and UI Elements: In the FortiGate GUI, SD-WAN zones that contain member interfaces are displayed with a plus (+) icon next to the checkbox. This icon allows administrators to expand the zone and view the specific physical or logical interfaces assigned to it.

Analysis of the "Underlay" Zone: In the provided exhibit, the virtual-wan-link and overlay zones both feature the plus (+) expansion icon, indicating they have active members. The Underlay zone, however, lacks this icon and displays a red status icon. This is the visual indicator in FortiOS that the zone is currently empty and contains no member interfaces.

Mandatory Zone Membership: In FortiOS 7.x, every SD-WAN member interface must be assigned to a

zone. It is not possible for an interface to be an "SD-WAN member" (as shown in the legend with port2 and port3) without being assigned to a zone. Since port2 and port3 are listed in the legend, they are indeed assigned to one of the other expanded zones (likely virtual-wan-link or overlay), making Option D incorrect.

Default Zone Behavior: While FortiOS 7.6 often creates default zones like virtual-wan-link, underlay, and overlay during certain configuration wizards or by default in newer versions, they are distinct entities.

There is no single "default" zone that acts as a global catch-all in the way Option C suggests.

Immutability of System Zones: While certain system-defined zones have restrictions, the primary focus of this specific exhibit is the current membership state, which clearly shows the Underlay zone is empty.

2.An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic. Which DPD mode on FortiGate meets this requirement?

- A. On Demand
- B. Enabled
- C. On Idle
- D. Usabled

Answer: A

Explanation:

Based on the FortiOS 7.6 Infrastructure and IPsec VPN documentation, Dead Peer Detection (DPD) can be configured in three primary modes: On Demand, On Idle, and Disabled.

On Demand (Default Mode): This mode is specifically designed to minimize unnecessary traffic. In this mode, FortiGate sends DPD probes only when there is no inbound traffic but the FortiGate is attempting to send outbound traffic. Because network communication is typically bidirectional, the absence of inbound traffic while outbound traffic is being sent is a primary indicator of a potentially dead tunnel. This matches the specific requirement described in the question.

On Idle: In this mode, DPD probes are sent if no traffic (neither inbound nor outbound) has been observed in the tunnel for a specific period. It verifies the tunnel status even when the connection is completely idle.

Enabled: In older versions or specific CLI contexts, "Enabled" may refer to periodic DPD, but in the current FortiOS 7.x/7.6 GUI and CLI terminology for Phase 1 settings, the active modes are defined as on-demand or on-idle.

Disabled: In this mode, the FortiGate does not send DPD probes but will still respond to DPD probes sent by the remote peer.

The requirement that the administrator wants probes sent only when there is no inbound traffic (usually implying the FortiGate is sending but not receiving) is the fundamental definition of the On Demand mechanism in the Fortinet curriculum.

3.Refer to the exhibit.

```

FortiGate # diagnose debug rating
Locale      : english

Service     : Web-filter
Status      : Enable
License     : Contract
\
Num. of servers : 1
Protocol    : https
Port        : 8888
Anycast     : Disable
Default servers : Not included

-- Server List (Wed Sep 20 09:22:42 2023) --

```

IP	Weight	RTT	Flags	TZ	FortiGuard-requests	Curr Lost	Total Lost	Updated Time
10.0.1.241	-244	2	I	0	122	0	0	Wed Sep 20 09:21:55 2023

Which two statements about the FortiGuard connection are true? (Choose two.)

- A. The weight increases as the number of failed packets rises
- B. You can configure unreliable protocols to communicate with FortiGuard Server.
- C. FortiGate identified the FortiGuard Server using DNS lookup.
- D. FortiGate is using the default port for FortiGuard communication.

Answer: A,D

Explanation:

Based on the diagnose debug rating output provided in the exhibit and the standard behavior of the FortiGuard connection mechanism in FortiOS 7.6:

Weight Calculation (Statement A is True):

In FortiOS, the rating server selection process uses a weight-based system.

According to official documentation, the weight increases with failed packets (lost responses) and decreases with successful packets.

This mechanism ensures that servers with poor reliability are penalized by having higher weights, effectively pushing them to the bottom of the preference list.

Default Port Communication (Statement D is True):

The exhibit explicitly shows the communication is using HTTPS on port 8888.

In FortiOS 7.6 (and legacy versions like 6.2/6.4), FortiGuard filtering supports specific protocols and ports: HTTPS on ports 443, 53, and 8888, where 8888 is considered a default port for FortiGuard queries.

Ports 53 and 8888 are standard for both UDP and TCP/HTTPS FortiGuard communications to avoid common firewall blocks on standard web ports.

Why other options are incorrect:

Statement B (Unreliable protocols): While you can configure UDP (which is unreliable), the exhibit specifically shows HTTPS is being used, which is a reliable (TCP-based) protocol.

Statement C (DNS lookup): In the "Flags" column of the server list, a server found via DNS lookup would be marked with the "D" flag. The exhibit shows the flag as "I" (indicating the last INIT request was sent to this server) and a numeric "2," but the "D" flag is absent. Additionally, the IP 10.0.1.241 is a private address, suggesting it is a manually configured FortiManager or local override server rather than a public server found via global DNS lookup.

4.What are two features of FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate uses the AD server as the collector agent.
- B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

- C. FortiGate does not support workstation check.
- D. FortiGate directs the collector agent to use a remote LDAP server.

Answer: B,C

Explanation:

Based on the FortiOS 7.6 Administrator Guide regarding Fortinet Single Sign-On (FSSO) polling modes, the agentless polling mode has specific technical characteristics:

SMB Protocol Usage (Statement B is True):

In agentless polling mode, the FortiGate unit itself acts as the collector.

It establishes direct connections to the Windows Domain Controllers (DCs) using the SMB (Server Message Block) protocol, typically over TCP port 445, to read the Windows Security Event logs.

This allows FortiGate to parse login event IDs (such as 4768 and 4769) to identify users and their corresponding IP addresses without needing an external collector agent installed on a server.

Workstation Check Support (Statement C is True):

One of the primary limitations of the agentless polling mode compared to the agent-based mode is the lack of workstation verification.

In agentless mode, FortiGate does not perform "workstation checks" or "dead entry checks". This means it cannot proactively verify if a user is still logged into a specific workstation after the initial logon event is recorded, which can lead to stale entries if a user logs off without a corresponding event being captured.

Why other options are incorrect:

Option A: In agentless mode, FortiGate (the FSSO daemon) performs the collection itself; it does not use the AD server as a "collector agent" in the functional sense of FSSO architecture.

Option D: While FortiGate uses LDAP to retrieve group membership information once a user is identified, it does not "direct" a collector agent to a remote LDAP server, as there is no external collector agent involved in this specific mode.

5.An administrator wants to form an HA cluster using the FGCP protocol.

Which two requirements must the administrator ensure both members fulfill? (Choose two.)

- A. They must have the same hard drive configuration.
- B. They must have the same number of configured VDOMs.
- C. They must have the heartbeat interfaces in the same subnet
- D. They must have the same HA group ID.

Answer: B,D

Explanation:

According to the FortiOS 7.6 High Availability (HA) Administration Guide and FGCP (FortiGate Clustering Protocol) requirements, the correct answers are B and D.

FGCP HA Cluster Mandatory Requirements (FortiOS 7.6)

When forming an HA cluster using FGCP, FortiGate devices must meet several strict compatibility and configuration requirements. Among the options given, the following two are mandatory:



- B. They must have the same number of configured VDOMs

In FortiOS HA, all cluster members must have the same VDOM configuration.

This includes:

Same number of VDOMs

Same VDOM names

This is required so configuration synchronization can occur correctly between members.

If VDOM counts differ, HA formation will fail.

✓ This is explicitly required and documented.



D. They must have the same HA group ID

The HA group ID uniquely identifies an HA cluster on the network.

All FortiGate units intended to join the same cluster must share the same HA group ID.

If the group IDs differ, devices will not recognize each other as cluster peers.

✓ This is a fundamental FGCP requirement.

Why the Other Options Are Incorrect



A. They must have the same hard drive configuration

Hard drive presence or size does not have to match for FGCP HA to function.

Disk differences may affect logging behavior, but they do not prevent HA cluster formation.

Therefore, this is not a required condition.



C. They must have the heartbeat interfaces in the same subnet Heartbeat interfaces must be:

Directly connected

In the same Layer 2 broadcast domain

They do not require IP addressing or being in the same IP subnet.

In many deployments, heartbeat interfaces have no IP addresses at all. Therefore, "same subnet" is not a documented requirement.