

# Fortinet NSE4\_FGT\_AD-7.6 Dumps with Practice Test Questions [2026]



ActualVCE is the website that provides all candidates with IT certification exam dumps and can help all candidates pass their exam with ease. ActualVCE IT expert edits all-time exam materials together on the basis of flexibly using the experiences of forefathers, thereby writing the best Fortinet NSE4\_FGT\_AD-7.6 Certification Training dumps. The exam dumps include all questions that can appear in the real exam. So it can guarantee you must pass your exam at the first time.

## Fortinet NSE4\_FGT\_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>• Routing: This domain covers configuring static routes for packet forwarding and implementing SD-WAN to load balance traffic across multiple WAN links.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>• Deployment and System Configuration: This domain covers initial FortiGate setup, logging configuration and troubleshooting, FGCP HA cluster configuration, resource and connectivity diagnostics, FortiGate cloud deployments (CNF and VM), and FortiSASE administration with user onboarding.</li></ul>
Topic 3	<ul style="list-style-type: none"><li>• Content Inspection: This domain addresses inspecting encrypted traffic using certificates, understanding inspection modes and web filtering, configuring application control, deploying antivirus scanning modes, and implementing IPS for threat protection.</li></ul>
Topic 4	<ul style="list-style-type: none"><li>• Firewall Policies and Authentication: This domain focuses on creating firewall policies, configuring SNAT and DNAT for address translation, implementing various authentication methods, and deploying FSSO for user identification.</li></ul>
Topic 5	<ul style="list-style-type: none"><li>• VPN: This domain focuses on implementing meshed or partially redundant IPsec VPN topologies for secure connections.</li></ul>

## Pass Guaranteed Efficient NSE4\_FGT\_AD-7.6 - Fortinet NSE 4 - FortiOS 7.6 Administrator Premium Exam

Our company pays high attentions to the innovation of our NSE4\_FGT\_AD-7.6 study materials. We constantly increase the investment on the innovation and build an incentive system for the members of the research expert team. Our experts group specializes in the research and innovation of our NSE4\_FGT\_AD-7.6 Study Materials and supplements the latest innovation and research results into the NSE4\_FGT\_AD-7.6 study materials timely.

### Fortinet NSE 4 - FortiOS 7.6 Administrator Sample Questions (Q125-Q130):

#### NEW QUESTION # 125

What are two characteristics of HA cluster heartbeat IP addresses in a FortiGate device?  
(Choose two.)

- A. The heartbeat interface of the primary device in the cluster is always assigned IP address 169.254.0.1.
- B. A change in the heartbeat IP address happens when a FortiGate device joins or leaves the cluster.
- C. Heartbeat IP addresses are used to distinguish between cluster members.
- D. Heartbeat interfaces have virtual IP addresses that are manually assigned.

**Answer: B,C**

Explanation:

The FGCP uses link-local IPv4 addresses (see RFC 3927) in the 169.254.0.x range for the virtual HA heartbeat interface (port\_ha) and for the inter-VDOM link interfaces between the vsys\_ha and management VDOM. When members join an HA cluster, each member's heartbeat interface (port\_ha) is assigned an IP address from the range of 169.254.0.1 to 169.254.0.63/26. HA inter-VDOM link interfaces (havdlink0 and havdlink1) are assigned IP address from the range of 169.254.0.65 to 169.254.0.66/26.

The IP address that is assigned to a virtual heartbeat interface depends on the serial number priority of the member. Higher serial numbers have a higher priority, and therefore a lower serialno\_prio number.

#### NEW QUESTION # 126

Which two statements describe how the RPF check is used? (Choose two.)

- A. The RPF check is run on the first sent packet of any new session.
- B. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.
- C. The RPF check is run on the first sent and reply packet of any new session.
- D. The RPF check is run on the first reply packet of any new session.

**Answer: A,B**

Explanation:

The RPF (Reverse Path Forwarding) check is used to prevent IP spoofing attacks by verifying that the source IP address of a received packet is reachable through the same interface it arrived on. If not, the packet is dropped, ensuring traffic legitimacy. The RPF check runs on the first sent packet of any new session to validate that the route to the source IP is consistent with the interface it's received on. This helps FortiGate detect spoofed or asymmetric routing scenarios early in the session establishment.

#### NEW QUESTION # 127

Refer to the exhibit. In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit.

What should the administrator do next, to troubleshoot the problem?



- A. Execute a debug flow.
- B. Execute another sniffer on FortiGate, this time with the filter "host 10.0.1.10".
- C. Run a sniffer on the web server.
- D. Capture the traffic using an external sniffer connected to port1.

**Answer: A**

Explanation:

The sniffer output shows that packets from the web client are reaching the FortiGate and being forwarded to the web server, but there is no indication that the web server is responding. To troubleshoot this issue, executing a debug flow will help analyze the traffic path and pinpoint where the problem might be occurring, such as a possible issue in firewall policy or route settings that is causing the server not to respond correctly.

#### NEW QUESTION # 128

Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true?  
(Choose two.)

- A. If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.
- B. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
- C. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.
- D. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP.

**Answer: A,C**

Explanation:

SD-WAN is enabled: v4-ecmp-mode is hide and you control the ECMP algorithm with the load-balance-mode setting.

SD-WAN is disabled: ECMP algorithm is set on the CLI: config system settings.

<https://docs.fortinet.com/document/fortigate/7.4.6/administration-guide/25967/equal-cost-multi-path>

#### NEW QUESTION # 129

Refer to the exhibits.

## Antivirus profile

### Edit AntiVirus Profile

Name

Comments  0/255

AntiVirus scan ☒ **Block** Monitor

Feature set ☐ Flow-based ☒ Proxy-based

Inspected Protocols

HTTP	<input checked="" type="checkbox"/>
SMTP	<input type="checkbox"/>
POP3	<input type="checkbox"/>
IMAP	<input type="checkbox"/>
FTP	<input checked="" type="checkbox"/>
CIFS	<input type="checkbox"/>
MAPI	<input checked="" type="checkbox"/>
SSH	<input checked="" type="checkbox"/>

## Firewall policy

### Edit Policy

Incoming interface

Outgoing interface

Source & Destination

Source

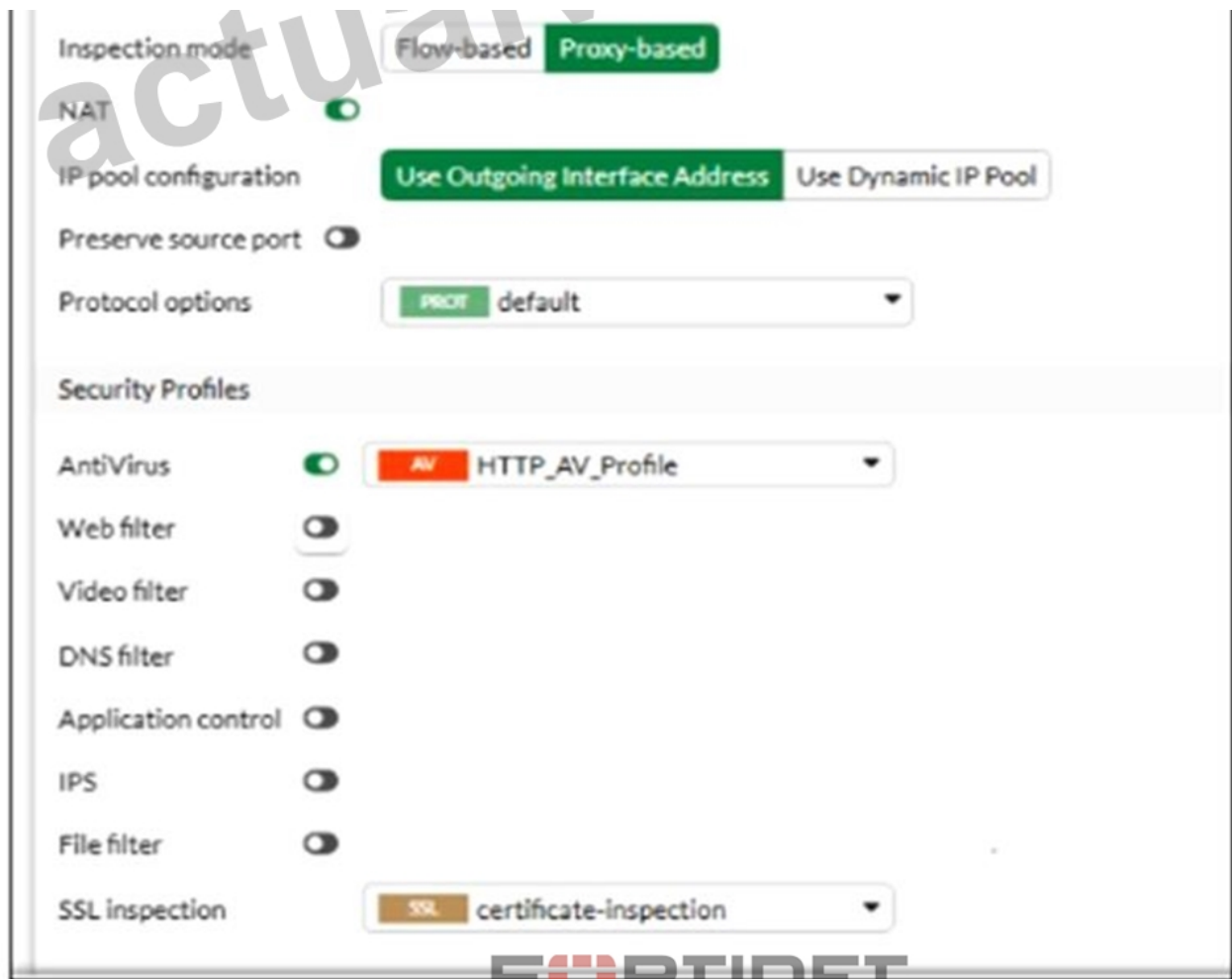
User/group

Destination

Service

<input checked="" type="checkbox"/> DNS	<input type="checkbox"/>
<input checked="" type="checkbox"/> HTTP	<input type="checkbox"/>
<input checked="" type="checkbox"/> HTTPS	<input type="checkbox"/>
<input checked="" type="checkbox"/> FTP	<input type="checkbox"/>

### Firewall/Network Options



## HTTPS access



You are asked to implement an antivirus profile for files downloaded through FTP, HTTP, and HTTPS. While testing, you are successful with HTTP and FTP protocols, but FortiGate does not block the file download over HTTPS. What could be the cause?

- A. The action on the firewall policy is not set to deny.
- B. The feature set in the antivirus profile is not set to Flow-based.
- C. The SSL inspection mode in the firewall policy is not deep content inspection.
- D. Web filter is not enabled on the firewall policy to complement the antivirus profile.

**Answer: C**

**Explanation:**

The SSL inspection mode in the firewall policy is set to certificate-inspection, which only examines SSL certificates without decrypting HTTPS traffic. Because of this, FortiGate cannot inspect or block files downloaded over HTTPS, as the content remains encrypted. To enable antivirus scanning on HTTPS traffic, the SSL inspection mode must be set to deep-inspection, allowing the FortiGate to decrypt, inspect, and re-encrypt the traffic.

• • • • •

**Latest NSE4\_FGT\_AD-7.6 Test Pdf:** [https://www.actualvce.com/Fortinet/NSE4\\_FGT\\_AD-7.6-valid-vce-dumps.html](https://www.actualvce.com/Fortinet/NSE4_FGT_AD-7.6-valid-vce-dumps.html)

- [illegible]