



## **Fortinet**

### **Exam Questions NSE4\_FGT-7.0**

Fortinet NSE 4 - FortiOS 7.0

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Exam Topic 1)

Refer to the exhibit.

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check. Which interface will be selected as an outgoing interface?

- A. port2
- B. port4
- C. port3
- D. port1

**Answer: D**

#### Explanation:

Port 1 shows the lowest latency.

### NEW QUESTION 2

- (Exam Topic 1)

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

- A. System time
- B. FortiGuard update servers
- C. Operating mode
- D. NGFW mode

**Answer: CD**

#### Explanation:

C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.

D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate\_Infrastructure\_6.4\_Study\_Guide

### NEW QUESTION 3

- (Exam Topic 1)

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

- \* All traffic must be routed through the primary tunnel when both tunnels are up
- \* The secondary tunnel must be used only if the primary tunnel goes down
- \* In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover

Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two,)

- A. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
- B. Enable Dead Peer Detection.
- C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
- D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

**Answer: BC**

#### Explanation:

B - because the customer requires the tunnels to notify when a tunnel goes down. DPD is designed for that purpose. To send a packet over a firewall to determine a failover for the next tunnel after a specific amount of time of not receiving a response from its peer.

C - remember when it comes to choosing a route with regards to Administrative Distance. The route with the lowest distance for that particular route will be chosen. So, by configuring a lower routing distance on the primary tunnel, means that the primary tunnel will be chosen to route packets towards their destination.

### NEW QUESTION 4

- (Exam Topic 1)

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

- A. The collector agent uses a Windows API to query DCs for user logins.
- B. NetAPI polling can increase bandwidth usage in large networks.
- C. The collector agent must search security event logs.
- D. The NetSession Enum function is used to track user logouts.

**Answer: D**

#### Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD34906>

<https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD34906&sliceId=1>

### NEW QUESTION 5

- (Exam Topic 1)

Refer to the exhibit.

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

- A. The port3 default route has the highest distance.
- B. The port3 default route has the lowest metric.
- C. There will be eight routes active in the routing table.
- D. The port1 and port2 default routes are active in the routing table.

**Answer:** AD

### NEW QUESTION 6

- (Exam Topic 1)

Which two statements about antivirus scanning mode are true? (Choose two.)

- A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
- B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
- C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
- D. In flow-based inspection mode, files bigger than the buffer size are scanned.

**Answer:** BC

#### Explanation:

An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM—something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

### NEW QUESTION 7

- (Exam Topic 1)

Refer to the web filter raw logs.

Based on the raw logs shown in the exhibit, which statement is correct?

- A. Social networking web filter category is configured with the action set to authenticate.
- B. The action on firewall policy ID 1 is set to warning.
- C. Access to the social networking web filter category was explicitly blocked to all users.
- D. The name of the firewall policy is all\_users\_web.

**Answer:** A

### NEW QUESTION 8

- (Exam Topic 1)

Which statement about video filtering on FortiGate is true?

- A. Full SSL Inspection is not required.
- B. It is available only on a proxy-based firewall policy.
- C. It inspects video files hosted on file sharing services.
- D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

**Answer:** B

#### Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/7.0.0/new-features/190873/video-filtering>

### NEW QUESTION 9

- (Exam Topic 1)

An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

- A. The strict RPF check is run on the first sent and reply packet of any new session.
- B. Strict RPF checks the best route back to the source using the incoming interface.
- C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
- D. Strict RPF allows packets back to sources with all active routes.

**Answer:** B

**Explanation:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955>

**NEW QUESTION 10**

- (Exam Topic 1)

Refer to the exhibit.

The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?

- A. Change password
- B. Enable restrict access to trusted hosts
- C. Change Administrator profile
- D. Enable two-factor authentication

**Answer:** C

**Explanation:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD34502>

**NEW QUESTION 10**

- (Exam Topic 1)

An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

- A. Policy lookup will be disabled.
- B. By Sequence view will be disabled.
- C. Search option will be disabled
- D. Interface Pair view will be disabled.

**Answer:** D

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821>

**NEW QUESTION 13**

- (Exam Topic 1)

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

- A. get system status
- B. get system performance status
- C. diagnose sys top
- D. get system arp

**Answer:** D

**Explanation:**

"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

**NEW QUESTION 14**

- (Exam Topic 1)

An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

- A. Add the support of NTLM authentication.
- B. Add user accounts to Active Directory (AD).
- C. Add user accounts to the FortiGate group filter.
- D. Add user accounts to the Ignore User List.

**Answer:** D

**Explanation:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828>

**NEW QUESTION 19**

- (Exam Topic 1)

Refer to the exhibit.

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

- A. Destination NAT is disabled in the firewall policy.
- B. One-to-one NAT IP pool is used in the firewall policy.

- C. Overload NAT IP pool is used in the firewall policy.
- D. Port block allocation IP pool is used in the firewall policy.

**Answer:** B

**Explanation:**

FortiGate\_Security\_6.4 page 155 . In one-to-one, PAT is not required.

**NEW QUESTION 22**

- (Exam Topic 1)

Refer to the exhibit.

Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

- A. There are five devices that are part of the security fabric.
- B. Device detection is disabled on all FortiGate devices.
- C. This security fabric topology is a logical topology view.
- D. There are 19 security recommendations for the security fabric.

**Answer:** CD

**Explanation:**

References: <https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results>

<https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology>

**NEW QUESTION 24**

- (Exam Topic 1)

Which two statements are true about the FGCP protocol? (Choose two.)

- A. Not used when FortiGate is in Transparent mode
- B. Elects the primary FortiGate device
- C. Runs only over the heartbeat links
- D. Is used to discover FortiGate devices in different HA groups

**Answer:** BC

**Explanation:**

Reference:

<https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/564712/fgcp-fortigate-clustering-protocol>

**NEW QUESTION 28**

- (Exam Topic 1)

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

- A. SSH
- B. HTTPS
- C. FTM
- D. FortiTelemetry

**Answer:** AB

**Explanation:**

Reference:

<https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/995103/buildingsecurity-into-fortios>

**NEW QUESTION 29**

- (Exam Topic 1)

FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.

Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

- A. www.example.com:443
- B. www.example.com
- C. example.com
- D. www.example.com/index.html

**Answer:** BC

**Explanation:**

FortiGate\_Security\_6.4 page 384

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names— "no URLs or wildcard characters are allowed".

**NEW QUESTION 32**

- (Exam Topic 1)

Refer to the exhibits.  
Exhibit A.

Exhibit B.

An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric. After synchronization, this object is not available on the downstream FortiGate (ISFW).

What must the administrator do to synchronize the address object?

- A. Change the csf setting on Local-FortiGate (root) to sec configuration-sync local.
- B. Change the csf setting on ISFW (downstream) to sec configuracion-sync local.
- C. Change the csf setting on Local-FortiGate (root) to sec fabric-objecc-unificacion defaultc.
- D. Change the csf setting on ISFW (downstream) to sec fabric-objecc-unificacion defaultc.

**Answer: A**

**Explanation:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD43820>

### NEW QUESTION 33

- (Exam Topic 1)

A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.

What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

- A. Static IP Address
- B. Dialup User
- C. Dynamic DNS
- D. Pre-shared Key

**Answer: B**

**Explanation:**

Dialup user is used when the remote peer's IP address is unknown. The remote peer whose IP address is unknown acts as the dialup client and this is often the case for branch offices and mobile VPN clients that use dynamic IP address and no dynamic DNS

### NEW QUESTION 38

- (Exam Topic 1)

Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

- A. The security actions applied on the web applications will also be explicitly applied on the third-party websites.
- B. The application signature database inspects traffic only from the original web application server.
- C. FortiGuard maintains only one signature of each web application that is unique.
- D. FortiGate can inspect sub-application traffic regardless where it was originated.

**Answer: D**

**Explanation:**

Reference:

[https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPX-AdminGuide/300\\_System/303d\\_FortiG](https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPX-AdminGuide/300_System/303d_FortiG)

### NEW QUESTION 43

- (Exam Topic 1)

Refer to the exhibit.

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster. Which two statements are true? (Choose two.)

- A. FortiGate SN FGVM010000065036 HA uptime has been reset.
- B. FortiGate devices are not in sync because one device is down.
- C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
- D. FortiGate SN FGVM010000064692 has the higher HA priority.

**Answer: AD**

**Explanation:**

\* 1. Override is disable by default - OK

\* 2. "If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the primary"

The question here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide.  
<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disab>

#### NEW QUESTION 44

- (Exam Topic 1)

Refer to the exhibit.

An administrator is running a sniffer command as shown in the exhibit.

Which three pieces of information are included in the sniffer output? (Choose three.)

- A. Interface name
- B. Ethernet header
- C. IP header
- D. Application header
- E. Packet payload

**Answer:** ACE

#### Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=11186>

#### NEW QUESTION 47

- (Exam Topic 2)

An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.16.1.0/24 and the remote quick mode selector is 192.16.2.0/24. How must the administrator configure the local quick mode selector for site B?

- A. 192.168.3.0/24
- B. 192.168.2.0/24
- C. 192.168.1.0/24
- D. 192.168.0.0/8

**Answer:** B

#### NEW QUESTION 51

- (Exam Topic 2)

An administrator must disable RPF check to investigate an issue.

Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

- A. Enable asymmetric routing, so the RPF check will be bypassed.
- B. Disable the RPF check at the FortiGate interface level for the source check.
- C. Disable the RPF check at the FortiGate interface level for the reply check.
- D. Enable asymmetric routing at the interface level.

**Answer:** B

#### Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955>

#### NEW QUESTION 54

- (Exam Topic 2)

Refer to the exhibit.

The exhibit contains a network interface configuration, firewall policies, and a CLI console configuration. How will FortiGate handle user authentication for traffic that arrives on the LAN interface?

- A. If there is a full-through policy in place, users will not be prompted for authentication.
- B. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.
- C. Authentication is enforced at a policy level; all users will be prompted for authentication.
- D. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

**Answer:** C

#### NEW QUESTION 55

- (Exam Topic 2)

Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate points the collector agent to use a remote LDAP server.

- B. FortiGate uses the AD server as the collector agent.
- C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- D. FortiGate queries AD by using the LDAP to retrieve user group information.

**Answer:** CD

**Explanation:**

Fortigate Infrastructure 7.0 Study Guide P.272-273 <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

**NEW QUESTION 56**

- (Exam Topic 2)

View the exhibit.

A user behind the FortiGate is trying to go to <http://www.addictinggames.com> (Addicting Games). Based on this configuration, which statement is true?

- A. Addicting.Games is allowed based on the Application Overrides configuration.
- B. Addicting.Games is blocked on the Filter Overrides configuration.
- C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
- D. Addcting.Games is allowed based on the Categories configuration.

**Answer:** A

**NEW QUESTION 59**

- (Exam Topic 2)

When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

- A. Log ID
- B. Universally Unique Identifier
- C. Policy ID
- D. Sequence ID

**Answer:** B

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies>

**NEW QUESTION 61**

- (Exam Topic 2)

Refer to the exhibit.

The exhibit contains a network diagram, firewall policies, and a firewall address object configuration.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-user2. Remote-user2 is still able to access Webserver.

Which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

- A. Disable match-vip in the Deny policy.
- B. Set the Destination address as Deny\_IP in the Allow-access policy.
- C. Enable match vip in the Deny policy.
- D. Set the Destination address as Web\_server in the Deny policy.

**Answer:** CD

**NEW QUESTION 62**

- (Exam Topic 2)

An administrator is running the following sniffer command:

Which three pieces of Information will be Included in me sniffer output? {Choose three.}

- A. Interface name
- B. Packet payload
- C. Ethernet header
- D. IP header
- E. Application header

**Answer:** ABD

**NEW QUESTION 64**

- (Exam Topic 2)

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

- A. FortiManager
- B. Root FortiGate
- C. FortiAnalyzer
- D. Downstream FortiGate

**Answer:** B

#### NEW QUESTION 66

- (Exam Topic 2)

A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) sub interfaces added to the physical interface. Which statements about the VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

- A. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.
- B. The two VLAN sub interfaces must have different VLAN IDs.
- C. The two VLAN sub interfaces can have the same VLAN ID, only if they belong to different VDOMs.
- D. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.

**Answer:** B

#### Explanation:

FortiGate\_Infrastructure\_6.0\_Study\_Guide\_v2-Online.pdf -> page 147

"Multiple VLANs can coexist in the same physical interface, provide they have different VLAN ID"

#### NEW QUESTION 70

- (Exam Topic 2)

Which feature in the Security Fabric takes one or more actions based on event triggers?

- A. Fabric Connectors
- B. Automation Stitches
- C. Security Rating
- D. Logical Topology

**Answer:** B

#### Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/286973/fortinet-security-fabric>

#### NEW QUESTION 74

- (Exam Topic 2)

Which two statements are correct about a software switch on FortiGate? (Choose two.)

- A. It can be configured only when FortiGate is operating in NAT mode
- B. Can act as a Layer 2 switch as well as a Layer 3 router
- C. All interfaces in the software switch share the same IP address
- D. It can group only physical interfaces

**Answer:** AC

#### NEW QUESTION 78

- (Exam Topic 2)

A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not. Which configuration option is the most effective way to support this request?

- A. Implement a web filter category override for the specified website
- B. Implement a DNS filter for the specified website.
- C. Implement web filter quotas for the specified website
- D. Implement web filter authentication for the specified website.

**Answer:** D

#### NEW QUESTION 80

- (Exam Topic 2)

Refer to the exhibit.

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.

Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

- A. On HQ-FortiGate, set IKE mode to Main (ID protection).
- B. On both FortiGate devices, set Dead Peer Detection to On Demand.
- C. On HQ-FortiGate, disable Diffie-Helman group 2.
- D. On Remote-FortiGate, set port2 as Interface.

**Answer:** AD

#### NEW QUESTION 82

- (Exam Topic 2)

Refer to the exhibit to view the firewall policy.

Which statement is correct if well-known viruses are not being blocked?

- A. The firewall policy does not apply deep content inspection.
- B. The firewall policy must be configured in proxy-based inspection mode.
- C. The action on the firewall policy must be set to deny.
- D. Web filter should be enabled on the firewall policy to complement the antivirus profile.

**Answer:** A

#### NEW QUESTION 87

- (Exam Topic 2)

Refer to the exhibit.

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration. The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IP address 10.0.1.254/24.

A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.

Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

- A. 10.200.1.149
- B. 10.200.1.1
- C. 10.200.1.49
- D. 10.200.1.99

**Answer:** D

#### NEW QUESTION 92

- (Exam Topic 2)

Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- A. diagnose wad session list
- B. diagnose wad session list | grep hook-pre&&hook-out
- C. diagnose wad session list | grep hook=pre&&hook=out
- D. diagnose wad session list | grep "hook=pre"&"hook=out"

**Answer:** A

#### NEW QUESTION 95

- (Exam Topic 2)

View the exhibit.

Which of the following statements are correct? (Choose two.)

- A. This setup requires at least two firewall policies with the action set to IPsec.
- B. Dead peer detection must be disabled to support this type of IPsec setup.
- C. The TunnelB route is the primary route for reaching the remote sit
- D. The TunnelA route is used only if the TunnelB VPN is down.
- E. This is a redundant IPsec setup.

**Answer:** CD

#### NEW QUESTION 99

- (Exam Topic 2)

What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

- A. FortiGate automatically negotiates different local and remote addresses with the remote peer.
- B. FortiGate automatically negotiates a new security association after the existing security association expires.
- C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
- D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

**Answer:** D

#### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=12069>

#### NEW QUESTION 100

- (Exam Topic 2)

Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

- A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
- B. ADVPN is only supported with IKEv2.
- C. Tunnels are negotiated dynamically between spokes.
- D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

**Answer:** AC

#### NEW QUESTION 103

- (Exam Topic 2)

Which of the following statements about central NAT are true? (Choose two.)

- A. IP tool references must be removed from existing firewall policies before enabling central NAT.
- B. Central NAT can be enabled or disabled from the CLI only.
- C. Source NAT, using central NAT, requires at least one central SNAT policy.
- D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

**Answer:** AB

#### NEW QUESTION 106

- (Exam Topic 2)

In which two ways can RPF checking be disabled? (Choose two )

- A. Enable anti-replay in firewall policy.
- B. Disable the RPF check at the FortiGate interface level for the source check
- C. Enable asymmetric routing.
- D. Disable strict-arc-check under system settings.

**Answer:** CD

#### Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955>

#### NEW QUESTION 107

- (Exam Topic 2)

Which two VDOMs are the default VDOMs created when FortiGate is set up in split VDOM mode? (Choose two.)

- A. FG-traffic
- B. Mgmt
- C. FG-Mgmt
- D. Root

**Answer:** AD

#### Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/758820/split-task-vdom-mode>

#### NEW QUESTION 111

- (Exam Topic 2)

An organization's employee needs to connect to the office through a high-latency internet connection. Which SSL VPN setting should the administrator adjust to prevent the SSL VPN negotiation failure?

- A. Change the session-ttl.
- B. Change the login timeout.
- C. Change the idle-timeout.
- D. Change the udp idle timer.

**Answer:** B

#### NEW QUESTION 112

- (Exam Topic 2)

In an explicit proxy setup, where is the authentication method and database configured?

- A. Proxy Policy
- B. Authentication Rule
- C. Firewall Policy
- D. Authentication scheme

**Answer:** D

#### NEW QUESTION 117

- (Exam Topic 2)

Which three methods are used by the collector agent for AD polling? (Choose three.)

- A. FortiGate polling
- B. NetAPI
- C. Novell API
- D. WMI
- E. WinSecLog

**Answer:** BDE

**Explanation:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

**NEW QUESTION 122**

- (Exam Topic 2)

If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

- A. The Services field prevents SNAT and DNAT from being combined in the same policy.
- B. The Services field is used when you need to bundle several VIPs into VIP groups.
- C. The Services field removes the requirement to create multiple VIPs for different services.
- D. The Services field prevents multiple sources of traffic from using multiple services to connect to a single computer.

**Answer: C**

**NEW QUESTION 127**

- (Exam Topic 2)

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?

- A. The browser requires a software update.
- B. FortiGate does not support full SSL inspection when web filtering is enabled.
- C. The CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.
- D. There are network connectivity issues.

**Answer: C**

**Explanation:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD41394>

**NEW QUESTION 132**

- (Exam Topic 2)

Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

- A. This is known as many-to-one NAT.
- B. Source IP is translated to the outgoing interface IP.
- C. Connections are tracked using source port and source MAC address.
- D. Port address translation is not used.

**Answer: BD**

**NEW QUESTION 135**

- (Exam Topic 2)

An administrator needs to increase network bandwidth and provide redundancy.

What interface type must the administrator select to bind multiple FortiGate interfaces?

- A. VLAN interface
- B. Software Switch interface
- C. Aggregate interface
- D. Redundant interface

**Answer: C**

**Explanation:**

Reference: <https://forum.fortinet.com/tm.aspx?m=120324>

**NEW QUESTION 138**

- (Exam Topic 2)

Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled on all FortiGate devices?

- A. Root VDOM
- B. FG-traffic VDOM
- C. Customer VDOM
- D. Global VDOM

**Answer: A**

**NEW QUESTION 143**

- (Exam Topic 2)

Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

- A. Log downloads from the GUI are limited to the current filter view
- B. Log backups from the CLI cannot be restored to another FortiGate.
- C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
- D. Log downloads from the GUI are stored as LZ4 compressed files.

**Answer:** AB

#### NEW QUESTION 147

- (Exam Topic 2)

Consider the topology:

Application on a Windows machine <--(SSL VPN)-->FGT--> Telnet to Linux server.

An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.

The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.

What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

- A. Set the maximum session TTL value for the TELNET service object.
- B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.
- C. Create a new service object for TELNET and set the maximum session TTL.
- D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

**Answer:** CD

#### NEW QUESTION 149

- (Exam Topic 2)

Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

- A. Subject Key Identifier value
- B. SMMIE Capabilities value
- C. Subject value
- D. Subject Alternative Name value

**Answer:** A

#### NEW QUESTION 151

- (Exam Topic 2)

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

- A. Warning
- B. Exempt
- C. Allow
- D. Learn

**Answer:** AC

#### NEW QUESTION 154

- (Exam Topic 2)

An administrator has configured a route-based IPsec VPN between two FortiGate devices. Which statement about this IPsec VPN configuration is true?

- A. A phase 2 configuration is not required.
- B. This VPN cannot be used as part of a hub-and-spoke topology.
- C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.
- D. The IPsec firewall policies must be placed at the top of the list.

**Answer:** C

#### Explanation:

In a route-based configuration, FortiGate automatically adds a virtual interface with the VPN name (Infrastructure Study Guide, 206)

#### NEW QUESTION 155

- (Exam Topic 2)

Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

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

**Answer:** BD

#### NEW QUESTION 157

- (Exam Topic 2)

Which of the following statements correctly describes FortiGate's route lookup behavior when searching for a suitable gateway? (Choose two)

- A. Lookup is done on the first packet from the session originator
- B. Lookup is done on the last packet sent from the responder
- C. Lookup is done on every packet, regardless of direction
- D. Lookup is done on the trust reply packet from the responder

**Answer:** AD

#### NEW QUESTION 161

- (Exam Topic 2)

Examine this FortiGate configuration:

Examine the output of the following debug command:

Based on the diagnostic outputs above, how is the FortiGate handling the traffic for new sessions that require inspection?

- A. It is allowed, but with no inspection
- B. It is allowed and inspected as long as the inspection is flow based
- C. It is dropped.
- D. It is allowed and inspected, as long as the only inspection required is antivirus.

**Answer: C**

#### NEW QUESTION 163

- (Exam Topic 2)

Which three statements about security associations (SA) in IPsec are correct? (Choose three.)

- A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.
- B. An SA never expires.
- C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.
- D. Phase 2 SA expiration can be time-based, volume-based, or both.
- E. Both the phase 1 SA and phase 2 SA are bidirectional.

**Answer: ACD**

#### NEW QUESTION 168

- (Exam Topic 2)

Refer to the exhibit.

According to the certificate values shown in the exhibit, which type of entity was the certificate issued to?

- A. A user
- B. A root CA
- C. A bridge CA
- D. A subordinate

**Answer: A**

#### NEW QUESTION 169

- (Exam Topic 2)

Which three statements are true regarding session-based authentication? (Choose three.)

- A. HTTP sessions are treated as a single user.
- B. IP sessions from the same source IP address are treated as a single user.
- C. It can differentiate among multiple clients behind the same source IP address.
- D. It requires more resources.
- E. It is not recommended if multiple users are behind the source NAT

**Answer: ACD**

#### NEW QUESTION 172

- (Exam Topic 2)

Refer to the exhibit to view the application control profile.

Users who use Apple FaceTime video conferences are unable to set up meetings. In this scenario, which statement is true?

- A. Apple FaceTime belongs to the custom monitored filter.
- B. The category of Apple FaceTime is being monitored.
- C. Apple FaceTime belongs to the custom blocked filter.
- D. The category of Apple FaceTime is being blocked.

**Answer: C**

#### NEW QUESTION 176

- (Exam Topic 2)

Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides (client and server) have terminated the session?

- A. To remove the NAT operation.
- B. To generate logs
- C. To finish any inspection operations.
- D. To allow for out-of-order packets that could arrive after the FIN/ACK packets.

**Answer: D**

**NEW QUESTION 177**

.....

## Relate Links

**100% Pass Your NSE4\_FGT-7.0 Exam with Exambible Prep Materials**

[https://www.exambible.com/NSE4\\_FGT-7.0-exam/](https://www.exambible.com/NSE4_FGT-7.0-exam/)

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>