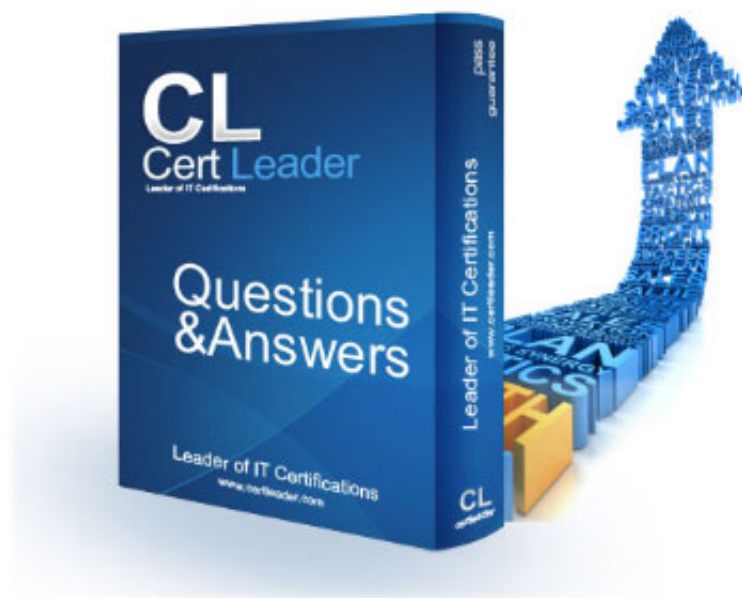


# NSE4\_FGT-7.0 Dumps

## Fortinet NSE 4 - FortiOS 7.0

[https://www.certleader.com/NSE4\\_FGT-7.0-dumps.html](https://www.certleader.com/NSE4_FGT-7.0-dumps.html)



**NEW QUESTION 1**

- (Exam Topic 1)

Refer to the exhibit.

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up. but phase 2 fails to come up.

Based on the phase 2 configuration shown in the exhibit, what configuration change will bring phase 2 up?

- A. On HQ-FortiGate, enable Auto-negotiate.
- B. On Remote-FortiGate, set Seconds to 43200.
- C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
- D. On HQ-FortiGate, set Encryption to AES256.

**Answer:** D

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/168495>

Encryption and authentication algorithm needs to match in order for IPSEC be successfully established.

**NEW QUESTION 2**

- (Exam Topic 1)

Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- A. FortiCache
- B. FortiSIEM
- C. FortiAnalyzer
- D. FortiSandbox
- E. FortiCloud

**Answer:** BCE

**Explanation:**

Reference:

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reporting-overview>

**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)

Which type of logs on FortiGate record information about traffic directly to and from the FortiGate management IP addresses?

A. System event logs

B. Forward traffic logs

C. Local traffic logs

D. Security logs

**Answer:** C

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/476970>

**NEW QUESTION 6**

- (Exam Topic 1)

Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

A. Proxy-based inspection

B. Certificate inspection

C. Flow-based inspection

D. Full Content inspection

**Answer:** AC

**NEW QUESTION 7**

- (Exam Topic 1)

Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

A. FortiGuard web filter cache

B. FortiGate hostname

C. NTP

D. DNS

**Answer:** CD

**NEW QUESTION 8**

- (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 9**

- (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)

Refer to the exhibit showing a debug flow output.

Which two statements about the debug flow output are correct? (Choose two.)

- A. The debug flow is of ICMP traffic.
- B. A firewall policy allowed the connection.
- C. A new traffic session is created.
- D. The default route is required to receive a reply.

**Answer:** AC

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/54688/debugging-the-packet-flow>

#### **NEW QUESTION 10**

- (Exam Topic 1)

Which three statements about a flow-based antivirus profile are correct? (Choose three.)

- A. IPS engine handles the process as a standalone.
- B. FortiGate buffers the whole file but transmits to the client simultaneously.
- C. If the virus is detected, the last packet is delivered to the client.
- D. Optimized performance compared to proxy-based inspection.
- E. Flow-based inspection uses a hybrid of scanning modes available in proxy-based inspection.

**Answer:** BDE

**Explanation:**

Reference: <https://forum.fortinet.com/tm.aspx?m=192309>

**NEW QUESTION 11**

- (Exam Topic 1)

Refer to the exhibits.

The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

- A. Change the SSL VPN port on the client.
- B. Change the Server IP address.
- C. Change the idle-timeout.
- D. Change the SSL VPN portal to the tunnel.

**Answer:** A

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/150494>

**NEW QUESTION 16**

- (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 20**

- (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 25**

- (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 27**

- (Exam Topic 1)

Refer to the exhibit.

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

- A. The session is in SYN\_SENT state.
- B. The session is in FIN\_ACK state.
- C. The session is in FTN\_WAIT state.
- D. The session is in ESTABLISHED state.

**Answer:** A

**Explanation:**

Indicates TCP (proto=6) session in SYN\_SENT state (proto=state=2) <https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

**NEW QUESTION 28**

- (Exam Topic 1)

Which statement about the policy ID number of a firewall policy is true?

- A. It is required to modify a firewall policy using the CLI.
- B. It represents the number of objects used in the firewall policy.
- C. It changes when firewall policies are reordered.
- D. It defines the order in which rules are processed.

**Answer:** A

**NEW QUESTION 33**

- (Exam Topic 1)

An administrator has configured the following settings:

What are the two results of this configuration? (Choose two.)

- A. Device detection on all interfaces is enforced for 30 minutes.
- B. Denied users are blocked for 30 minutes.
- C. A session for denied traffic is created.

D. The number of logs generated by denied traffic is reduced.

**Answer:** CD

**Explanation:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46328>

#### **NEW QUESTION 37**

- (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 38**

- (Exam Topic 1)

Which two statements are correct about NGFW Policy-based mode? (Choose two.)

- A. NGFW policy-based mode does not require the use of central source NAT policy
- B. NGFW policy-based mode can only be applied globally and not on individual VDOMs
- C. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy
- D. NGFW policy-based mode policies support only flow inspection

**Answer:** CD

#### **NEW QUESTION 40**

- (Exam Topic 1)

Which two statements about SSL VPN between two FortiGate devices are true? (Choose two.)

- A. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.

- B. The client FortiGate requires a manually added route to remote subnets.
- C. The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VPN.
- D. Server FortiGate requires a CA certificate to verify the client FortiGate certificate.

**Answer:** CD

**Explanation:**

Reference:

<https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/266506/ssl-vpn-with-certificate-authentication>

**NEW QUESTION 44**

- (Exam Topic 1)

A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded.

What is the reason for the failed virus detection by FortiGate?

- A. Application control is not enabled
- B. SSL/SSH Inspection profile is incorrect
- C. Antivirus profile configuration is incorrect
- D. Antivirus definitions are not up to date

**Answer:** B

**Explanation:**

https traffic requires SSL decryption. Check the ssh inspection profile

**NEW QUESTION 45**

- (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 50**

- (Exam Topic 2)

Which two statements are true when FortiGate is in transparent mode? (Choose two.)

- A. By default, all interfaces are part of the same broadcast domain.
- B. The existing network IP schema must be changed when installing a transparent mode.
- C. Static routes are required to allow traffic to the next hop.
- D. FortiGate forwards frames without changing the MAC address.

**Answer:** AD

**Explanation:**

Reference: [https://kb.fortinet.com/kb/viewAttachment.do?](https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113)

[attachID=Fortigate\\_Transparent\\_Mode\\_Technical\\_Guide\\_FortiOS\\_4\\_0\\_version1.2.pdf&documentID=FD33113](https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113)

**NEW QUESTION 53**

- (Exam Topic 2)



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 as shown in the exhibit.

What should the administrator do next to troubleshoot the problem?

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

**Answer: D**

#### **NEW QUESTION 54**

- (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 59**

- (Exam Topic 2)

An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

- A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
- B. Create a new service object for HTTP service and set the session TTL to never
- C. Set the TTL value to never under config system-ttl

D. Set the session TTL on the HTTP policy to maximum

**Answer:** BC

#### NEW QUESTION 62

- (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 67

- (Exam Topic 2)

Examine this PAC file configuration.

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

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.
- B. Any web request to the 172.25.120.0/24 subnet is allowed to bypass the proxy.
- C. All requests not made to Fortinet.com or the 172.25.120.0/24 subnet, have to go through altproxy.corp.com: 8060.
- D. Any web request fortinet.com is allowed to bypass the proxy.

**Answer:** AD

#### NEW QUESTION 69

- (Exam Topic 2)

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

- A. To detect intermediary NAT devices in the tunnel path.
- B. To dynamically change phase 1 negotiation mode aggressive mode.
- C. To encapsulation ESP packets in UDP packets using port 4500.
- D. To force a new DH exchange with each phase 2 rekey.

**Answer:** AC

#### NEW QUESTION 74

- (Exam Topic 2)

If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

- A. A CRL
- B. A person
- C. A subordinate CA
- D. A root CA

**Answer:** D

**NEW QUESTION 78**

- (Exam Topic 2)

Which two statements are true about the RPF check? (Choose two.)

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

**Answer:** AD

**Explanation:**

Reference: <https://www.programmersought.com/article/16383871634/>

**NEW QUESTION 82**

- (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 83**

- (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 85**

- (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 89**

- (Exam Topic 2)

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

- A. Configure Source IP Pools.

- B. Configure split tunneling in tunnel mode.
- C. Configure different SSL VPN realms.
- D. Configure host check.

**Answer:** D

**NEW QUESTION 92**

- (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 95**

- (Exam Topic 2)

Refer to the exhibit, which contains a session diagnostic output.

Which statement is true about the session diagnostic output?

- A. The session is a UDP unidirectional state.
- B. The session is in TCP ESTABLISHED state.
- C. The session is a bidirectional UDP connection.
- D. The session is a bidirectional TCP connection.

**Answer:** C

**NEW QUESTION 100**

- (Exam Topic 2)

Which of statement is true about SSL VPN web mode?

- A. The tunnel is up while the client is connected.
- B. It supports a limited number of protocols.
- C. The external network application sends data through the VPN.
- D. It assigns a virtual IP address to the client.

**Answer:** B

**Explanation:**

FortiGate\_Security\_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

**NEW QUESTION 103**

- (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 107

- (Exam Topic 2)

Which two statements about IPsec authentication on FortiGate are correct? (Choose two.)

- A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password
- B. FortiGate supports pre-shared key and signature as authentication methods.
- C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.
- D. A certificate is not required on the remote peer when you set the signature as the authentication method.

**Answer:** AB

#### Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/913287/ipsec-vpn-authenticating-aremote-fortigate>

#### NEW QUESTION 111

- (Exam Topic 2)

Refer to the exhibit to view the application control profile.

Based on the configuration, what will happen to Apple FaceTime?

- A. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration
- B. Apple FaceTime will be allowed, based on the Apple filter configuration.
- C. Apple FaceTime will be allowed only if the filter in Application and Filter Overrides is set to Learn
- D. Apple FaceTime will be allowed, based on the Categories configuration.

**Answer:** A

#### NEW QUESTION 112

- (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 115

- (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 116

- (Exam Topic 2)

Refer to the exhibit.

The exhibit shows proxy policies and proxy addresses, the authentication rule and authentication scheme, users, and firewall address.

An explicit web proxy is configured for subnet range 10.0.1.0/24 with three explicit web proxy policies. The authentication rule is configured to authenticate HTTP requests for subnet range 10.0.1.0/24 with a form-based authentication scheme for the FortiGate local user database. Users will be prompted for authentication.

How will FortiGate process the traffic when the HTTP request comes from a machine with the source IP 10.1.1.10 to the destination <http://www.fortinet.com>? (Choose two.)

- A. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.
- B. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.
- C. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.
- D. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

**Answer:** BD

#### NEW QUESTION 120

- (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 121

- (Exam Topic 2)

Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

- A. diagnose sys top
- B. execute ping
- C. execute traceroute
- D. diagnose sniffer packet any
- E. get system arp

**Answer:** BCD

#### NEW QUESTION 125

- (Exam Topic 2)

Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

- A. The public key of the web server certificate must be installed on the browser.
- B. The web-server certificate must be installed on the browser.
- C. The CA certificate that signed the web-server certificate must be installed on the browser.
- D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

**Answer:** C

#### NEW QUESTION 128

- (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 131

- (Exam Topic 2)

Refer to the exhibit.

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?

- A. Custom permission for Network
- B. Read/Write permission for Log & Report
- C. CLI diagnostics commands permission
- D. Read/Write permission for Firewall

**Answer:** C

#### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220>

#### NEW QUESTION 135

- (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 138

- (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 140**

- (Exam Topic 2)

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

- A. SMTP.Login.Brute.Force
- B. IMAP.Login.brute.Force
- C. ip\_src\_session
- D. Location: server Protocol: SMTP

**Answer:** B

#### **NEW QUESTION 141**

- (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 144**

- (Exam Topic 2)

Which statement regarding the firewall policy authentication timeout is true?

- A. It is an idle timeou
- B. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source IP.
- C. It is a hard timeou
- D. The FortiGate removes the temporary policy for a user’s source IP address after this timer has expired.
- E. It is an idle timeou
- F. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source MAC.
- G. It is a hard timeou
- H. The FortiGate removes the temporary policy for a user’s source MAC address after this timer has expired.



**Answer:** A

**NEW QUESTION 145**

- (Exam Topic 2)

Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.

An administrator has configured the WINDOWS\_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic. What is a possible reason for this?

- A. The IPS filter is missing the Protocol: HTTPS option.
- B. The HTTPS signatures have not been added to the sensor.
- C. A DoS policy should be used, instead of an IPS sensor.
- D. A DoS policy should be used, instead of an IPS sensor.
- E. The firewall policy is not using a full SSL inspection profile.

**Answer:** E

**NEW QUESTION 147**

- (Exam Topic 2)

Which two statements are true about the Security Fabric rating? (Choose two.)

- A. It provides executive summaries of the four largest areas of security focus.
- B. Many of the security issues can be fixed immediately by clicking Apply where available.
- C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
- D. The Security Fabric rating is a free service that comes bundled with all FortiGate devices.

**Answer:** BC

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/292634/security-rating>

**NEW QUESTION 152**

- (Exam Topic 2)

Which three authentication timeout types are available for selection on FortiGate? (Choose three.)

- A. hard-timeout

- B. auth-on-demand
- C. soft-timeout
- D. new-session
- E. Idle-timeout

**Answer:** ADE

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221>

**NEW QUESTION 153**

- (Exam Topic 2)

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scanning of application traffic to the DNS protocol only.
- B. It limits the scanning of application traffic to use parent signatures only.
- C. It limits the scanning of application traffic to the browser-based technology category only.
- D. It limits the scanning of application traffic to the application category only.

**Answer:** C

**NEW QUESTION 155**

- (Exam Topic 2)

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

- A. The interface has been configured for one-arm sniffer.
- B. The interface is a member of a virtual wire pair.
- C. The operation mode is transparent.
- D. The interface is a member of a zone.
- E. Captive portal is enabled in the interface.

**Answer:** ABC

**Explanation:**

[https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top\\_VirtualWirePair.htm](https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm)

**NEW QUESTION 160**

- (Exam Topic 2)

Which scanning technique on FortiGate can be enabled only on the CLI?

- A. Heuristics scan
- B. Trojan scan
- C. Antivirus scan
- D. Ransomware scan

**Answer:** A

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/567568/enabling-scanning>

**NEW QUESTION 163**

- (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 166**

- (Exam Topic 2)

An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must an administrator do to achieve this objective?

- A. The administrator can register the same FortiToken on more than one FortiGate.
- B. The administrator must use a FortiAuthenticator device.
- C. The administrator can use a third-party radius OTP server.
- D. The administrator must use the user self-registration server.

**Answer:** B

**NEW QUESTION 167**

- (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 170**

- (Exam Topic 2)

Refer to the exhibit.

The exhibits show a network diagram and the explicit web proxy configuration.

In the command diagnose sniffer packet, what filter can you use to capture the traffic between the client and the explicit web proxy?

- A. 'host 192.168.0.2 and port 8080'
- B. 'host 10.0.0.50 and port 80'
- C. 'host 192.168.0.1 and port 80'
- D. 'host 10.0.0.50 and port 8080'

**Answer:** A

**NEW QUESTION 171**

- (Exam Topic 2)

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporally disabled while upgrading the firmware.

**Answer:** CD

**NEW QUESTION 172**

- (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 174**

- (Exam Topic 2)

Examine the following web filtering log.

Which statement about the log message is true?

- A. The action for the category Games is set to block.
- B. The usage quota for the IP address 10.0.1.10 has expired
- C. The name of the applied web filter profile is default.
- D. The web site miniclip.com matches a static URL filter whose action is set to Warning.

**Answer:** C

**NEW QUESTION 177**

- (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 180**

- (Exam Topic 2)

What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

- A. Full Content inspection
- B. Proxy-based inspection
- C. Certificate inspection
- D. Flow-based inspection

**Answer:** D

**NEW QUESTION 182**

- (Exam Topic 2)

Refer to the exhibit, which contains a static route configuration.

An administrator created a static route for Amazon Web Services. What CLI command must the administrator use to view the route?

- A. get router info routing-table all
- B. get internet service route list
- C. get router info routing-table database
- D. diagnose firewall proute list

**Answer:** D

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortigate/latest/administration-guide/139692/routing-concepts>

**NEW QUESTION 187**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your NSE4\_FGT-7.0 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/NSE4\\_FGT-7.0-dumps.html](https://www.certleader.com/NSE4_FGT-7.0-dumps.html)