



Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

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)

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 3

- (Exam Topic 1)

An administrator wants to configure timeouts for users. Regardless of the user's behavior, the timer should start as soon as the user authenticates and expire after the configured value.

Which timeout option should be configured on FortiGate?

- A. auth-on-demand
- B. soft-timeout
- C. idle-timeout
- D. new-session
- E. hard-timeout

Answer: E

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221#:~:text=Hard%20timeout%3A%20User%20>

NEW QUESTION 4

- (Exam Topic 1)

Refer to the exhibit.

The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies 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. The first firewall policy has NAT enabled using IP Pool.

The second firewall policy is configured with a VIP as the destination address.

Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0.1.10?

- A. 10.200.1.1
- B. 10.200.3.1

- C. 10.200.1.100
- D. 10.200.1.10

Answer: A

Explanation:

Reference:

<https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-firewall/Concepts%20-%20Firewall/Static%20N>

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD44529>

NEW QUESTION 5

- (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 cast 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 6

- (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 7

- (Exam Topic 1)

When configuring a firewall virtual wire pair policy, which following statement is true?

- A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
- B. Only a single virtual wire pair can be included in each policy.
- C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
- D. Exactly two virtual wire pairs need to be included in each policy.

Answer: A

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD48690>

NEW QUESTION 8

- (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 9

- (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 10

- (Exam Topic 1)

Refer to the exhibits.

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook.

Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

- A. The SSL inspection needs to be a deep content inspection.
- B. Force access to Facebook using the HTTP service.
- C. Additional application signatures are required to add to the security policy.
- D. Add Facebook in the URL category in the security policy.

Answer: A

Explanation:

The lock logo behind Facebook_like.Button indicates that SSL Deep Inspection is Required.

NEW QUESTION 10

- (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 15

- (Exam Topic 2)

View the exhibit:

Which the FortiGate handle web proxy traffic rue? (Choose two.)

- A. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.
- B. port-VLAN1 is the native VLAN for the port1 physical interface.
- C. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
- D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

Answer: AC

NEW QUESTION 20

- (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?>

attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113

NEW QUESTION 24

- (Exam Topic 2)

Refer to the FortiGuard connection debug output.

Based on the output shown in the exhibit, which two statements are correct? (Choose two.)

- A. A local FortiManager is one of the servers FortiGate communicates with.
- B. One server was contacted to retrieve the contract information.
- C. There is at least one server that lost packets consecutively.
- D. FortiGate is using default FortiGuard communication settings.

Answer: BD

NEW QUESTION 27

- (Exam Topic 2)

You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk. What is the default behavior when the local disk is full?

- A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.
- B. No new log is recorded until you manually clear logs from the local disk.
- C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.
- D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

Answer: C

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.4.0/cli-reference/462620/log-disk-setting>

NEW QUESTION 28

- (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 29

- (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 31

- (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 34

- (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 35

- (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 38

- (Exam Topic 2)

NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

- A. Web filtering
- B. Antivirus
- C. Web proxy
- D. Application control

Answer: B

NEW QUESTION 42

- (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 47

- (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 51

- (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 55

- (Exam Topic 2)

If Internet Service is already selected as Destination in a firewall policy, which other configuration objects can be selected to the Destination field of a firewall policy?

A User or User Group

- A. IP address
- B. No other object can be added
- C. FQDN address

Answer: B

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy>

NEW QUESTION 56

- (Exam Topic 2)

Refer to the exhibit, which contains a radius server configuration.

An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.

What will be the impact of using Include in every user group option in a RADIUS configuration?

- A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
- B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
- C. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.
- D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Answer: A

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/634373/authentication-servers>

NEW QUESTION 58

- (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 59

- (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 64

- (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 68

- (Exam Topic 2)

Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

- A. Source defined as Internet Services in the firewall policy.
- B. Destination defined as Internet Services in the firewall policy.
- C. Highest to lowest priority defined in the firewall policy.
- D. Services defined in the firewall policy.
- E. Lowest to highest policy ID number.

Answer: ABD

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47435>

NEW QUESTION 72

- (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 77

- (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 82

- (Exam Topic 2)

Refer to the exhibit.

The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses.

How does FortiGate process the traffic sent to <http://www.fortinet.com>?

- A. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 3.
- B. Traffic will not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.
- C. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 1.
- D. Traffic will be redirected to the transparent proxy and it will be denied by the proxy implicit deny policy.

Answer: D

NEW QUESTION 84

- (Exam Topic 2)

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

- A. By default, FortiGate uses WINS servers to resolve names.
- B. By default, the SSL VPN portal requires the installation of a client's certificate.
- C. By default, split tunneling is enabled.
- D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer: D

NEW QUESTION 88

- (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 89

- (Exam Topic 2)

Which statement regarding the firewall policy authentication timeout is true?

- A. It is an idle timeout
- 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 timeout
- D. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
- E. It is an idle timeout
- 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 timeout
- H. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Answer: A

NEW QUESTION 93

- (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 96

- (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 98

- (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

NEW QUESTION 101

- (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 105

- (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 106

- (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 temporarily disabled while upgrading the firmware.

Answer: CD

NEW QUESTION 108

- (Exam Topic 2)

Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

- A. Shut down/reboot a downstream FortiGate device.
- B. Disable FortiAnalyzer logging for a downstream FortiGate device.
- C. Log in to a downstream FortiSwitch device.
- D. Ban or unban compromised hosts.

Answer: AB

NEW QUESTION 112

- (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 113

- (Exam Topic 2)

When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

- A. remote user's public IP address
- B. The public IP address of the FortiGate device.
- C. The remote user's virtual IP address.
- D. The internal IP address of the FortiGate device.

Answer: D

Explanation:

Source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address

NEW QUESTION 114

- (Exam Topic 2)

How do you format the FortiGate flash disk?

- A. Load a debug FortiOS image.
- B. Load the hardware test (HQIP) image.
- C. Execute the CLI command execute formatlogdisk.
- D. Select the format boot device option from the BIOS menu.

Answer: D

NEW QUESTION 115

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE4_FGT-7.0 Practice Exam Features:

- * NSE4_FGT-7.0 Questions and Answers Updated Frequently
- * NSE4_FGT-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4_FGT-7.0 Practice Test Here](#)