NSE4_FGT-7.2 Q&As

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse4_fgt-7-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 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

Correct Answer: CD

In the 7.2 Infrastructure Guide (page 306) the list of configuration settings that are NOT synchronized includes both \\'FortiGate host name\\' and \\'Cache\\'

QUESTION 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

Correct Answer: B

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

QUESTION 3

An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings.

What is true about the DNS connection to a FortiGuard server?

A. It uses UDP 8888.

B. It uses UDP 53.

C. It uses DNS over HTTPS.

D. It uses DNS overTLS.

Correct Answer: D

FortiGate Security 7.2 Study Guide (p.15): "When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT)

by default to secure the DNS traffic."

When using FortiGuard servers for DNS, FortiOS defaults to using DNS over TLS (DoT) to secure the DNS traffic1. DNS over TLS is a protocol that encrypts and authenticates DNS queries and responses using the Transport Layer Security (TLS) protocol2. This prevents eavesdropping, tampering, and spoofing of DNS data by third parties. The default FortiGuard DNS servers are 96.45.45.45 and 96.45.46.46, and they use the hostname globalsdns.fortinet.net1. The FortiGate verifies the server hostname using the server-hostname setting in the system dns configuration1.

QUESTION 4

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

Correct Answer: BC

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.

OK: google.com or www.google.com

NO OK: www.google.com/index.html or google.*

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".

QUESTION 5

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.

Correct Answer: AD

Reference: https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdfanddo cumentID=FD33113

QUESTION 6

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

A. IP address

B. Once Internet Service is selected, no other object can be added

C. User or User Group

D. FQDN address

Correct Answer: B

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

QUESTION 7

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

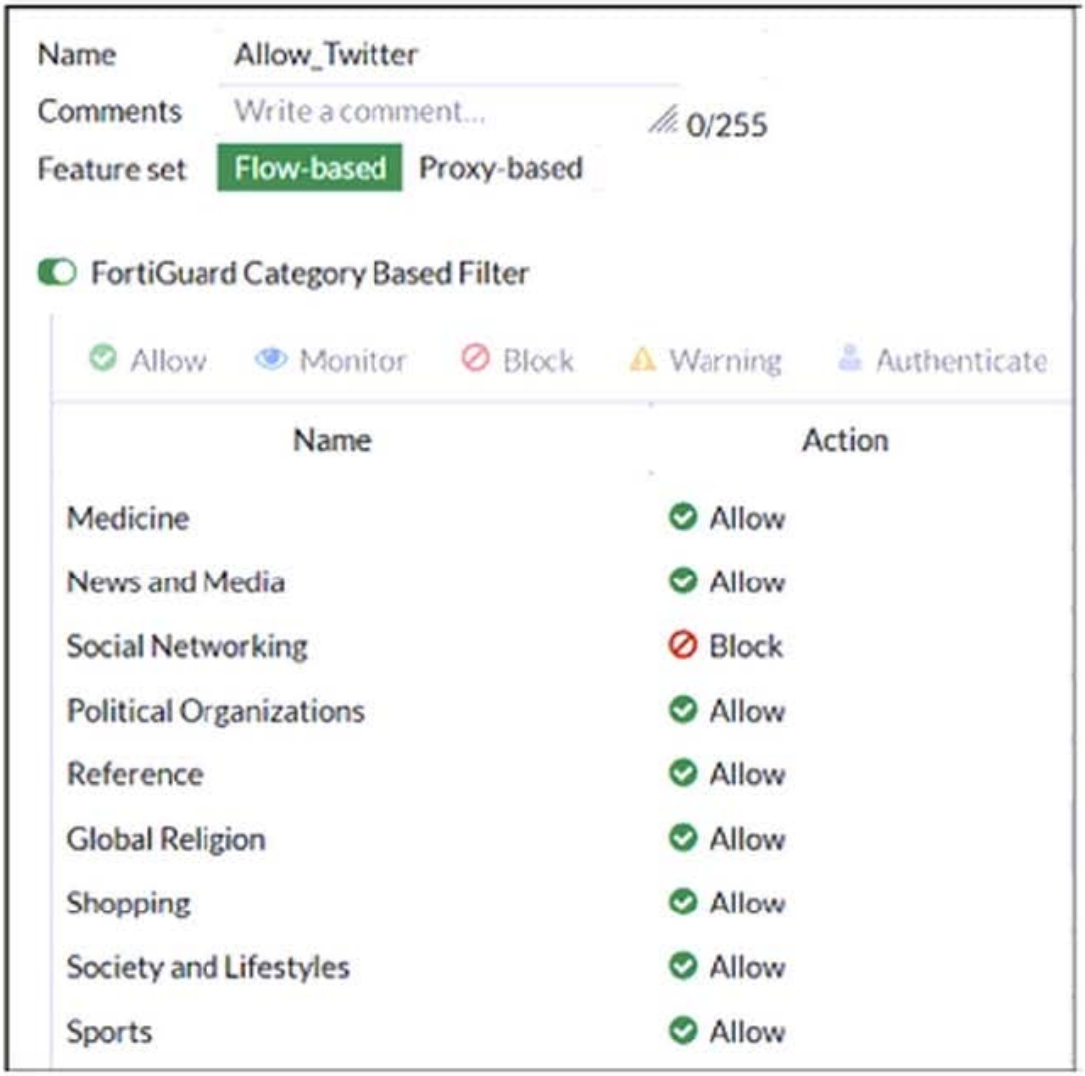
D. Learn

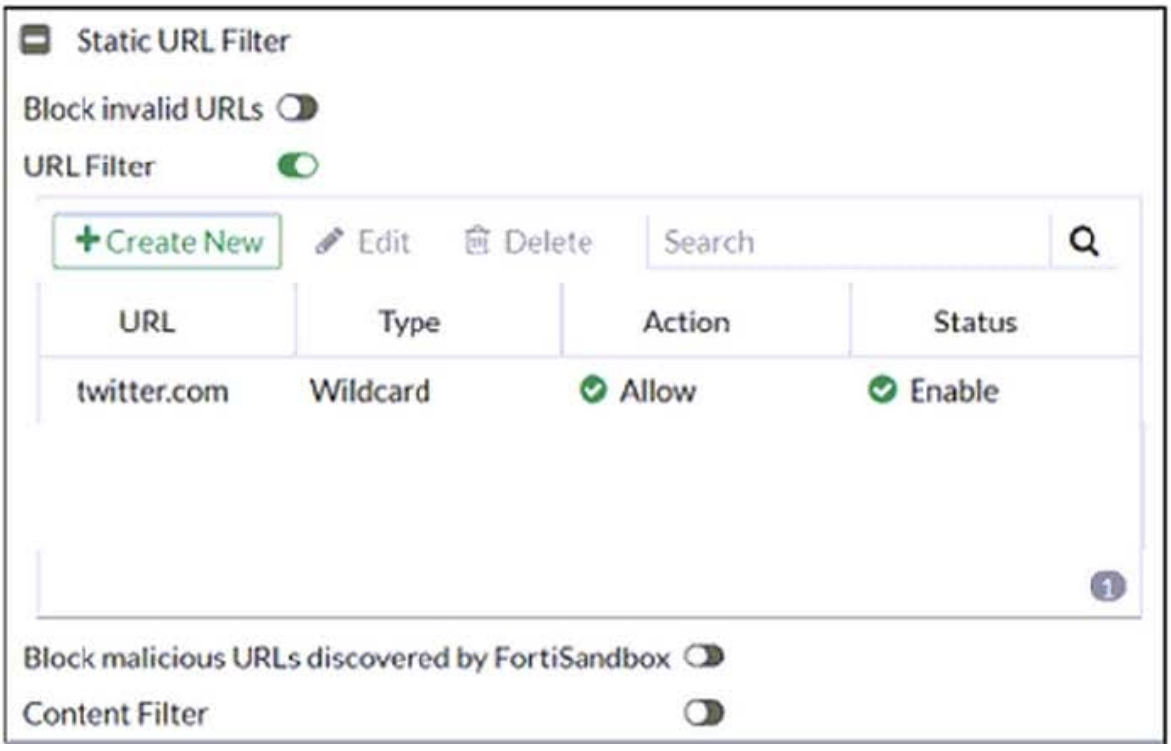
Correct Answer: AC

QUESTION 8

Refer to exhibit.

An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.


Name
Allow_Twitter
Comments
Write a comment...
0/255
Feature set
Flow-based
Proxy-based
FortiGuard Category Based Filter
Allow
Monitor
Block
Warning
Authenticate
Name
Action
Medicine
Allow
News and Media
Allow
Social Networking
Block
Political Organizations
Allow
Reference
Allow
Global Religion
Allow
Shopping
Allow
Society and Lifestyles
Allow
Sports
Allow


Static URL Filter
Block invalid URLs
URL Filter
Create New
Edit
Delete
Search
URL
Type
Action
Status
twitter.com
Wildcard
Allow
Enable
Block malicious URLs discovered by FortiSandbox
Content Filter

Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

A. On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking

B. On the Static URL Filter configuration, set Type to Simple

C. On the Static URL Filter configuration, set Action to Exempt.

D. On the Static URL Filter configuration, set Action to Monitor.

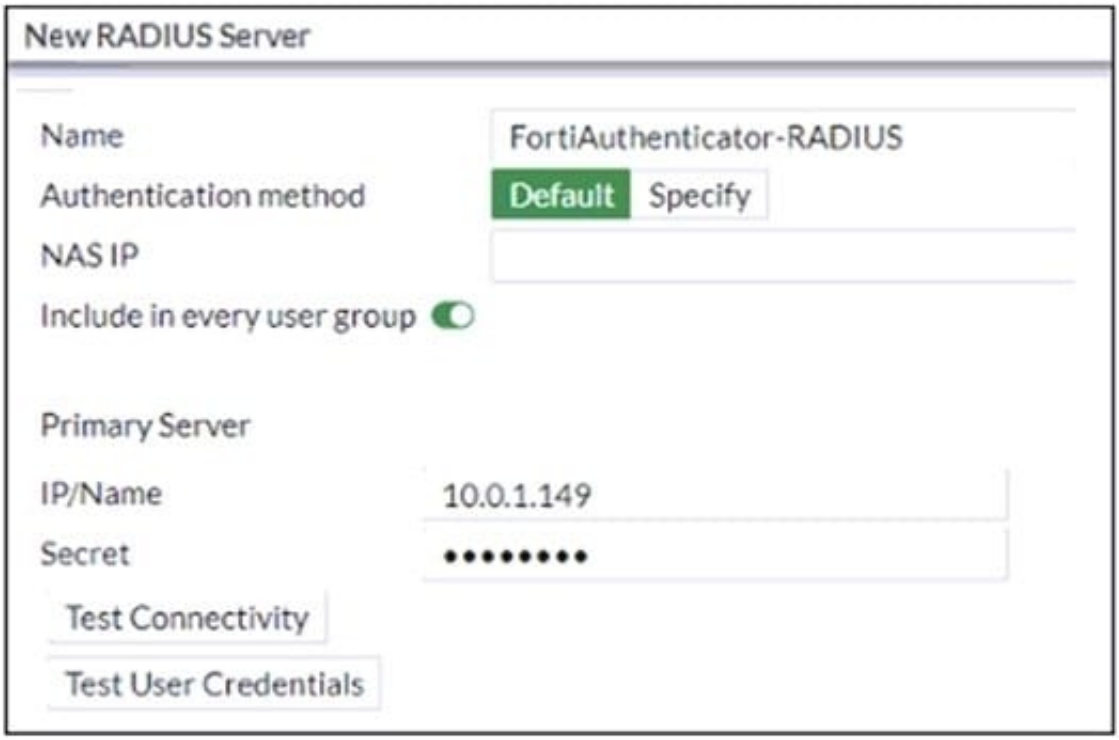
Correct Answer: C

Reference: https://fortinet77.rssing.com/chan-56127603/article113.html Based on the exhibit, the administrator has configured the FortiGuard Category Based Filter to block access to all social networking sites, and has also configured a Static URL Filter to block access to twitter.com. As a result, users are being redirected to a block page when they try to access twitter.com. To allow users to access twitter.com while blocking all other social networking sites, the administrator can make the following configuration change: On the Static URL Filter configuration, set Action to Exempt: By setting the Action to Exempt, the administrator can override the block on twitter.com that was specified in the FortiGuard Category Based Filter. This will allow users to access twitter.com, while all other social networking sites will still be blocked.

QUESTION 9

Refer to the exhibit.

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



What is the impact of using the 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.

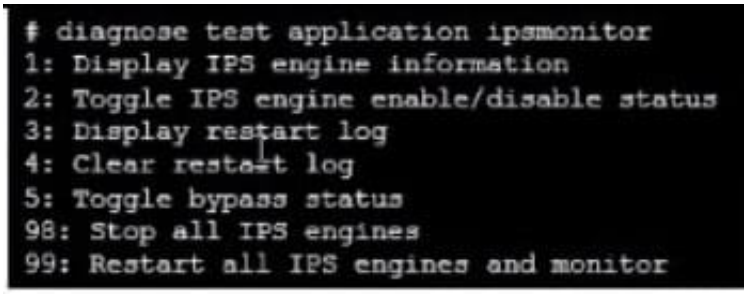
D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Correct Answer: A

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

QUESTION 10

Refer to the exhibit.



Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

A. The IPS engine was inspecting high volume of traffic.

B. The IPS engine was unable to prevent an intrusion attack .

C. The IPS engine was blocking all traffic.

D. The IPS engine will continue to run in a normal state.

Correct Answer: A

fortinet-fortigate-security-study-guide-for-fortios-72 page 417 If there are high-CPU use problems caused by the IPS, you can use the diagnose test application ipsmonitor command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

Reference: https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/232929/troubleshooting-high-cpu-usage

QUESTION 11

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.

Correct Answer: CD

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

QUESTION 12

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

A. hard-timeout

B. auth-on-demand

C. soft-timeout

D. new-session

E. Idle-timeout

Correct Answer: ADE

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

QUESTION 13

Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not provide any data integrity or encryption.

B. AH does not support perfect forward secrecy.

C. AH provides data integrity bur no encryption.

D. AH provides strong data integrity but weak encryption.

Correct Answer: C

QUESTION 14

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

A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

B. The RPF check is run on the first sent and reply packet of any new session.

C. The RPF check is run on the first sent packet of any new session.

D. The RPF check is run on the first reply packet of any new session.

Correct Answer: AC

FortiGate Infrastructure 7.2 Study Guide (p.41): "The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table." "FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn\\'t perform any additional RPF checks on that session."

A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks. This is true because the RPF check verifies that the source IP address of an incoming packet matches the reverse route for that address, meaning that the packet came from a legitimate source and not from an attacker who is trying to impersonate another host. This prevents IP spoofing attacks, where an attacker sends packets with a forged source IP address to bypass security policies or launch denial-of-service attacks1 C. The RPF check is run on the first sent packet of any new session. This is true because the RPF check is performed only once per session, on the first packet sent by either the client or the server, depending on the direction of the session initiation. This reduces the processing overhead and improves performance2

QUESTION 15

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.

Correct Answer: B

FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.