Free Questions for NSE4_FGT-7.2 by ebraindumps

Shared by Andrews on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the web filter raw logs.

Image not found or type unknown

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

Options:

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

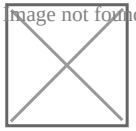
Question 2

Question Type: MultipleChoice

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?

Options:

A) Change the csf setting on Local-FortiGate (root) to set configuration-sync local.

B) Change the csf setting on ISFW (downstream) to set configuration-sync local.

C) Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.

D) Change the csf setting on ISFW (downstream) to set fabric-object-unification default.

Answer:

C

Question 3

Question Type: MultipleChoice

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

Options:

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:

https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPX-AdminGuide/300_System/303d_FortiG

Question 4

Question Type: MultipleChoice

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?

Options:

A) Change the session-ttl.

B) Change the login timeout.

C) Change the idle-timeout.

D) Change the udp idle timer.

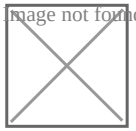
Answer:

B

Question 5

Question Type: **MultipleChoice**

Refer to the FortiGuard connection debug output.



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

Options:

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:

B, D

Question 6

Question Type: **MultipleChoice**

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.

Options:

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'

Question 7

Question Type: **MultipleChoice**

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?

Options:

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