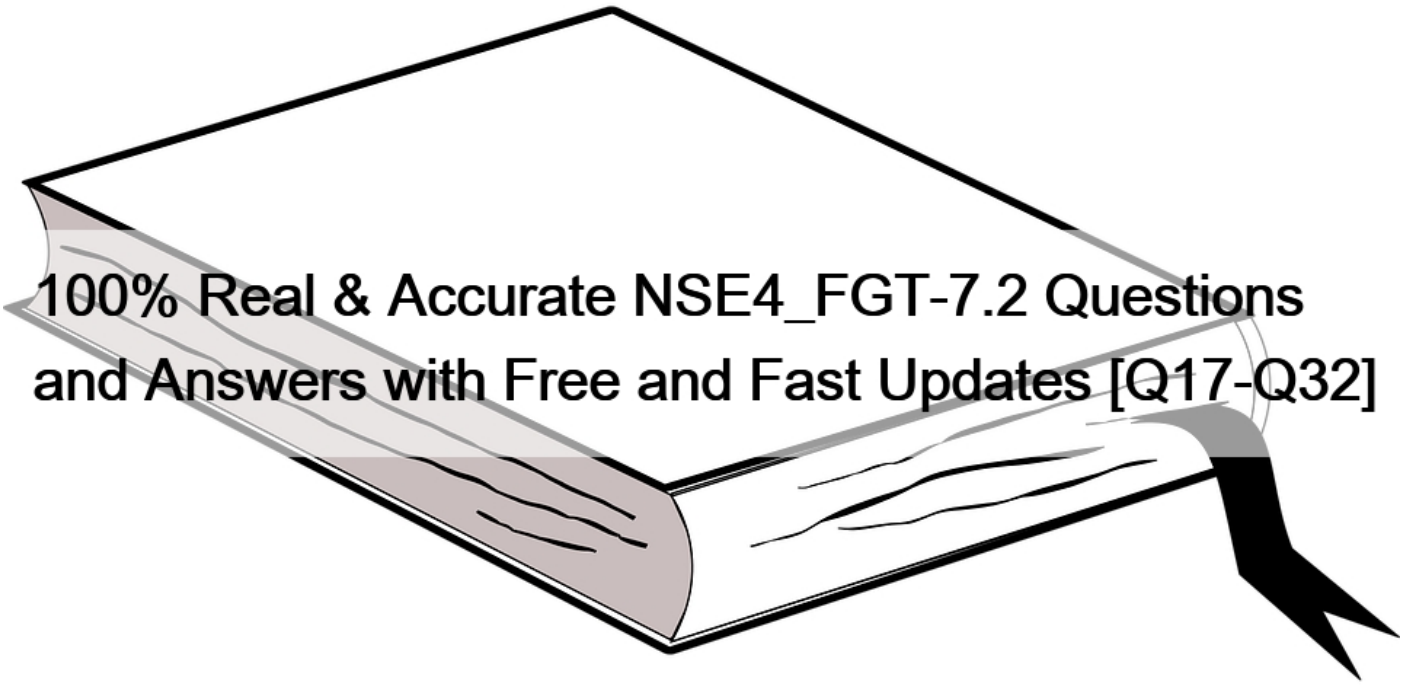
100% Real & Accurate NSE4_FGT-7.2 Questions and Answers with Free and Fast Updates [Q17-Q32



100% Real & Accurate NSE4_FGT-7.2 Questions and Answers with Free and Fast Updates
Get Unlimited Access to NSE4_FGT-7.2 Certification Exam Cert Guide

NEW QUESTION 17

An administrator is running the following sniffer command:

Which three pieces of Information will be Included in me sniffer output? {Choose three.)
* Interface name
* Packet payload
* Ethernet header
* IP header
* Application header

NEW QUESTION 18

Refer to the web filter raw logs.

Based on the raw logs shown in the exhibit, which statement is correct?
* Social networking web filter category is configured with the action set to authenticate.
* The action on firewall policy ID 1 is set to warning.
* Access to the social networking web filter category was explicitly blocked to all users.
* The name of the firewall policy is all_users_web.

NEW QUESTION 19

Which statement about the IP authentication header (AH) used by IPsec is true?
* AH does not provide any data integrity or encryption.
* AH does not support perfect forward secrecy.
* AH provides data integrity bur no encryption.
* AH provides strong data integrity but weak encryption.

NEW QUESTION 20

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.)
* www.example.com:443
* www.example.com
* example.com
* www.example.com/index.html

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”.

NEW QUESTION 21

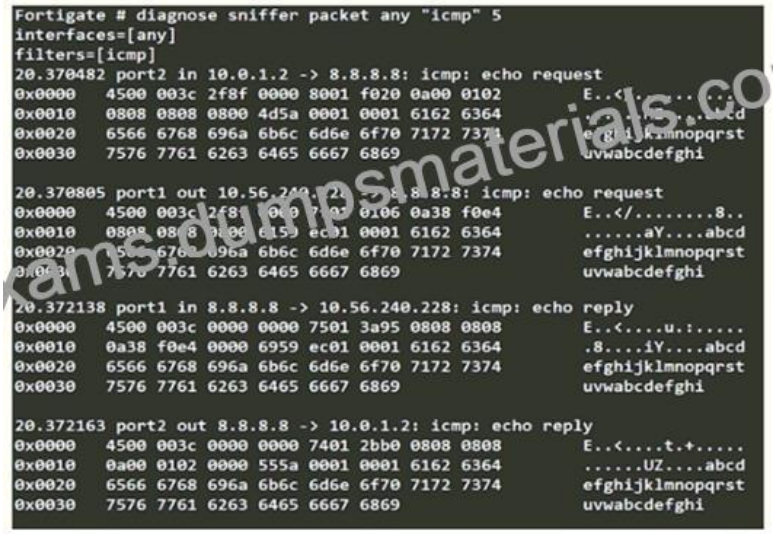
A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.

What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?
* Static IP Address
* Dialup User
* Dynamic DNS
* Pre-shared Key

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 clien and this is often the case for branch offices and mobile VPN clients that use dynamic IP address and no dynamic DNS

NEW QUESTION 22

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.)
* Interface name
* Ethernet header

* IP header
* Application header
* Packet payload

Reference:

Study Guide – Routing – Diagnostics – Packet Capture Verbosity Level.

diagnose sniffer packet <interface> ‘<filter>’ <verbosity> <count> <timestamp> <frame size> In the example, verbosity is 5.

The verbosity level specifies how much info you want to display.

1 (default): IP Headers.

2: IP Headers, Packet Payload.

3. IP Headers, Packet Payload, Ethernet Headers.

4: IP Headers, Interface Name.

5: IP Headers, Packet Payload, Interface Name.

6: IP Headers, Packet Payload, Ethernet Headers, Interface Name.

NEW QUESTION 23

Which three statements explain a flow-based antivirus profile? (Choose three.)

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

NEW QUESTION 24

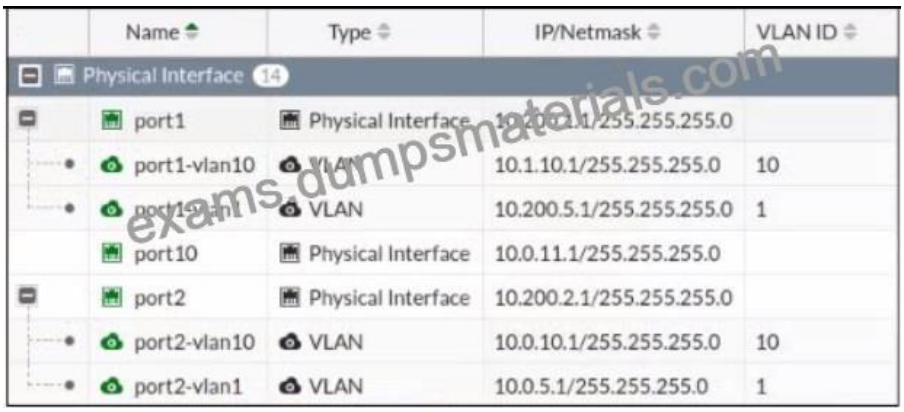
Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

* hard-timeout
* auth-on-demand
* soft-timeout
* new-session
* Idle-timeout

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

NEW QUESTION 25

Refer to the exhibit.



	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)
* Traffic between port2 and port2-vlan1 is allowed by default.
* port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
* port1 is a native VLAN.
* port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf

https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883

NEW QUESTION 26

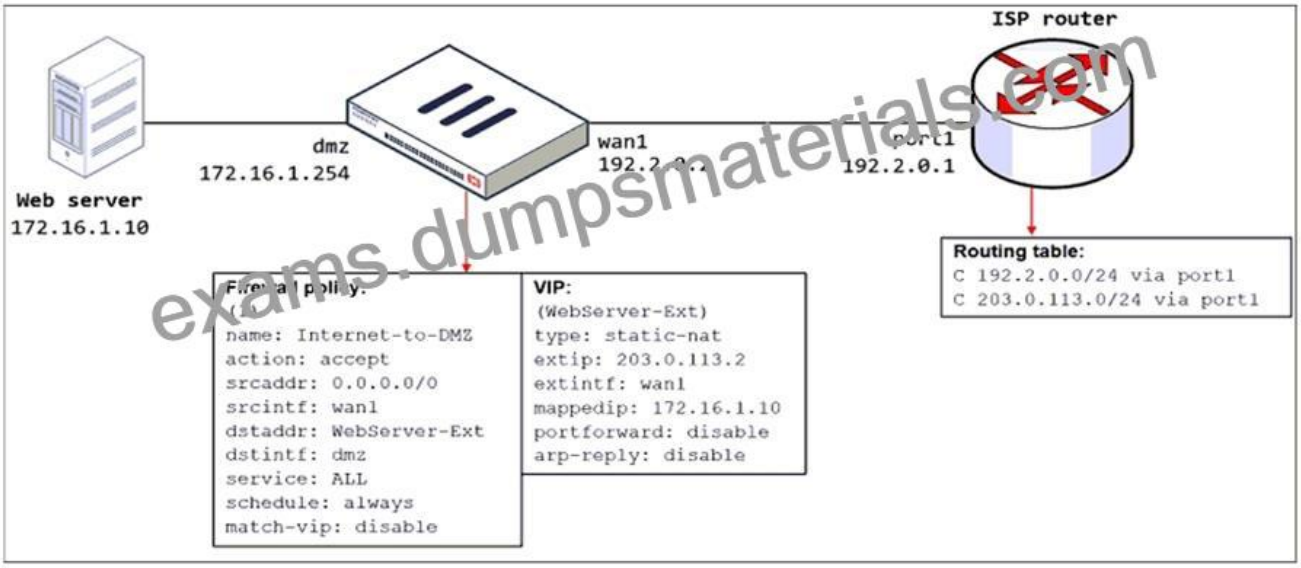
A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not Which configuration option is the most effective way to support this request?
* Implement a web filter category override for the specified website
* Implement a DNS filter for the specified website.
* Implement web filter quotas for the specified website
* Implement web filter authentication for the specified website.

NEW QUESTION 27

Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.

When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.



Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

* Configure a loopback interface with address 203.0.113.2/32.
* In the VIP configuration, enable arp-reply.
* Enable port forwarding on the server to map the external service port to the internal service port.
* In the firewall policy configuration, enable match-vip.

NEW QUESTION 28

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?

* IP address
* Once Internet Service is selected, no other object can be added
* User or User Group
* FQDN address

Reference:

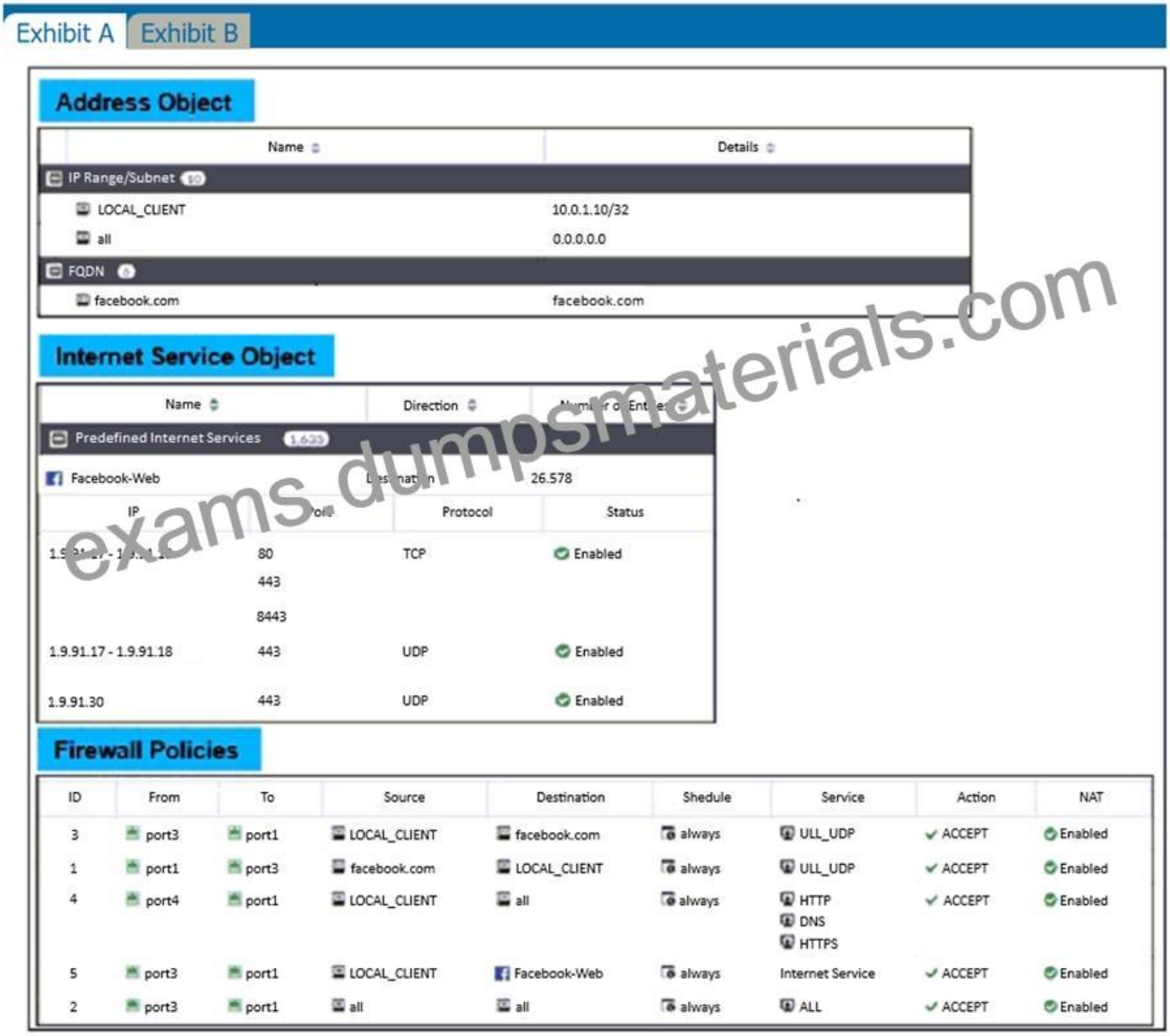
https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy

NEW QUESTION 29

Refer to the exhibits.

The exhibits show the firewall policies and the objects used in the firewall policies.

The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.



Which policy will be highlighted, based on the input criteria?

* Policy with ID 4.
* Policy with ID 5.
* Policies with ID 2 and 3.
* Policy with ID 4.

NEW QUESTION 30

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?

* Enable asymmetric routing, so the RPF check will be bypassed.
* Disable the RPF check at the FortiGate interface level for the source check.
* Disable the RPF check at the FortiGate interface level for the reply check .

* Enable asymmetric routing at the interface level.

NEW QUESTION 31

Refer to the exhibit.

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)
* The port3 default route has the highest distance.
* The port3 default route has the lowest metric.
* There will be eight routes active in the routing table.
* The port1 and port2 default routes are active in the routing table.

NEW QUESTION 32

Which statement regarding the firewall policy authentication timeout is true?
* It is an idle timeout. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source IP.
* It is a hard timeout. The FortiGate removes the temporary policy for a user’s source IP address after this timer has expired.
* It is an idle timeout. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source MAC.
* It is a hard timeout. The FortiGate removes the temporary policy for a user’s source MAC address after this timer has expired.