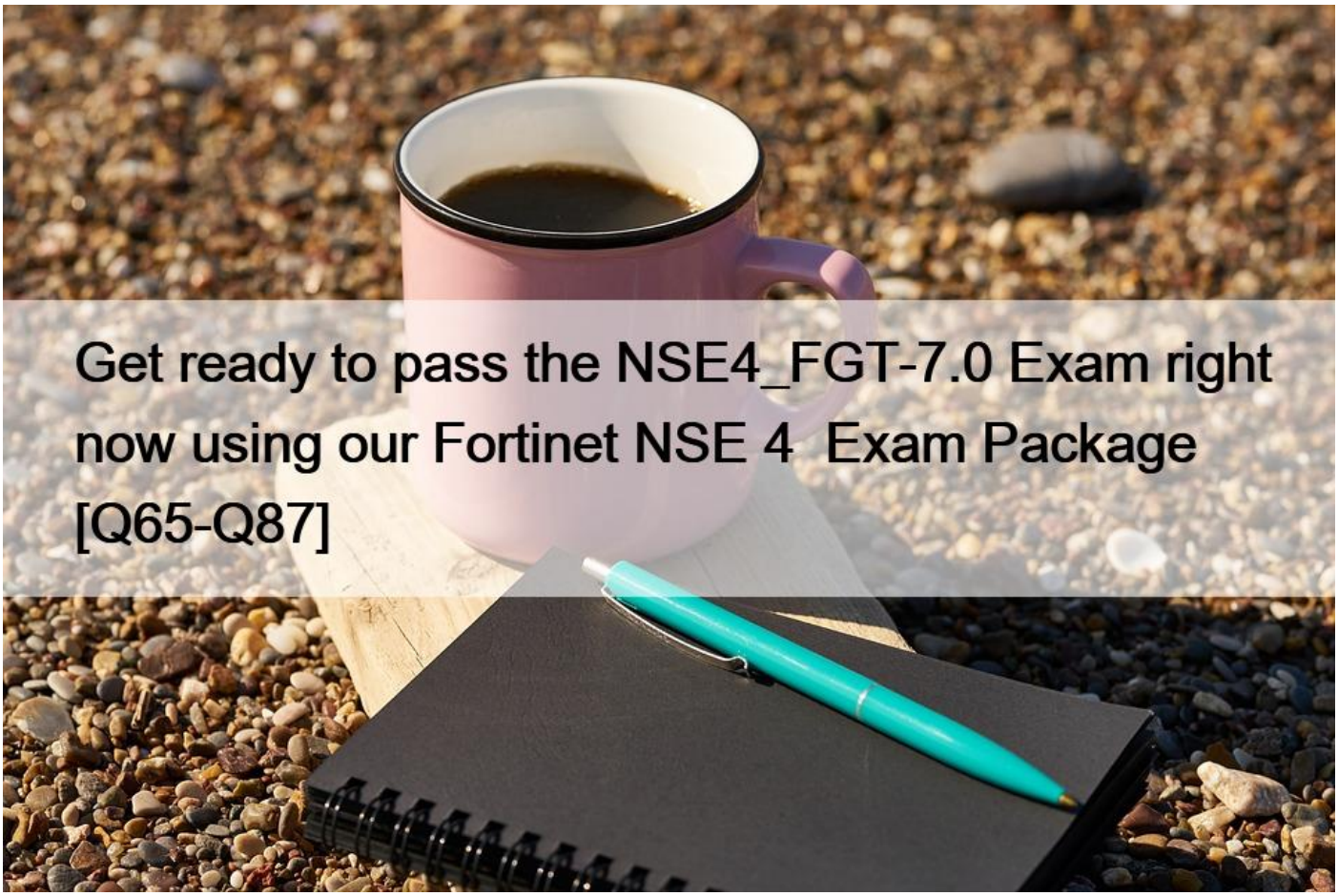
Get ready to pass the NSE4_FGT-7.0 Exam right now using our Fortinet NSE 4 Exam Package [Q65-Q87



Get ready to pass the NSE4_FGT-7.0 Exam right now using our Fortinet NSE 4 Exam Package
A fully updated 2022 NSE4_FGT-7.0 Exam Dumps exam guide from training expert Exams4sures

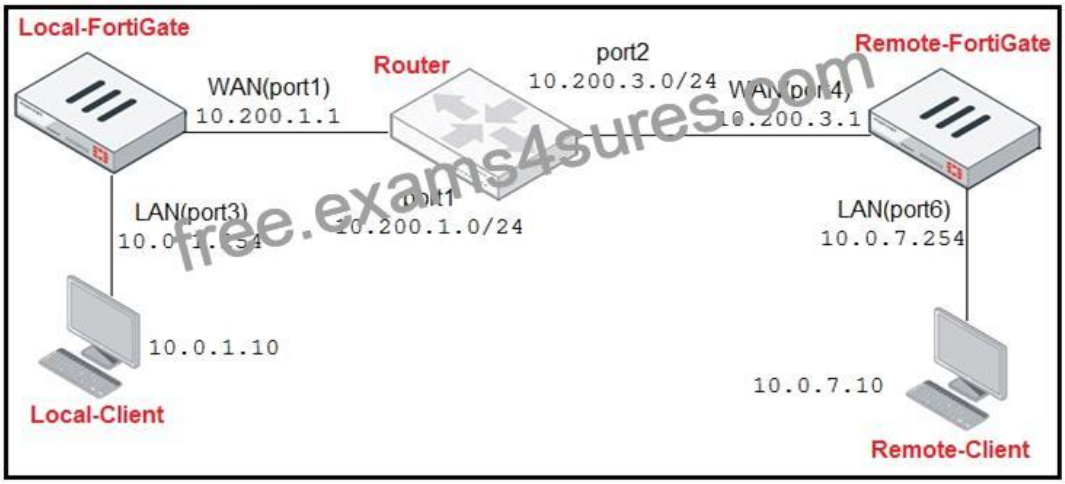
Fortinet NSE4_FGT-7.0 Exam Syllabus Topics:

TopicDetailsTopic 1- Identify and configure different methods of firewall authentication- Describe and inspect encrypted traffic using certificatesTopic 2- Explain and configure antivirus scanning modes to neutralize malware threats- Identify FortiGate inspection modes and configure web and DNS filteringTopic 3- Configure IPS, DoS, and WAF to protect the network from hacking and DDoS attacks- Configure log settings and diagnose problems using the logsTopic 4- Configure and route packets using static and policy-based routes- Identify and configure different operation modes for an FGCP HA cluster

QUESTION 65

Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

Create New | Edit | Delete | Search

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate

Create New | Edit | Clone | Delete | Search

Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	Enabled

Protocol Number Table

Protocol Number Table	
Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

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.

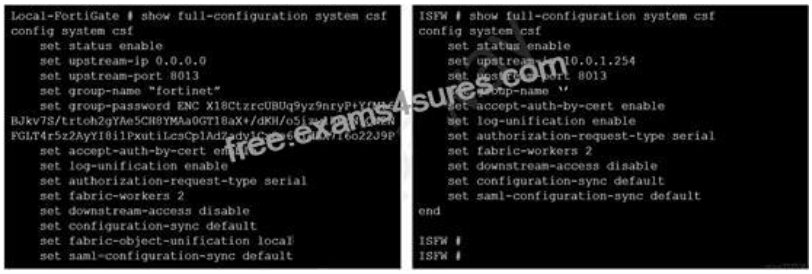
Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?
* 10.200.1.149
* 10.200.1.1
* 10.200.1.49
* 10.200.1.99

QUESTION 66

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?
* Change the csf setting on Local-FortiGate (root) to sec configuration-sync local.
* Change the csf setting on ISFW (downstream) to sec configuracion-sync local.
* Change the csf setting on Local-FortiGate (root) to sec fabric-objecc-unificacion defaulc.
* Change the csf setting on ISFW (downstream) to sec fabric-objecc-unificacion defaulc.

QUESTION 67

What is the primary FortiGate election process when the HA override setting is disabled?
* Connected monitored ports > System uptime > Priority > FortiGate Serial number
* Connected monitored ports > HA uptime > Priority > FortiGate Serial number
* Connected monitored ports > Priority > HA uptime > FortiGate Serial number
* Connected monitored ports > Priority > System uptime > FortiGate Serial number

QUESTION 68

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)
* SSH
* HTTPS
* FTM
* FortiTelemetry

QUESTION 69

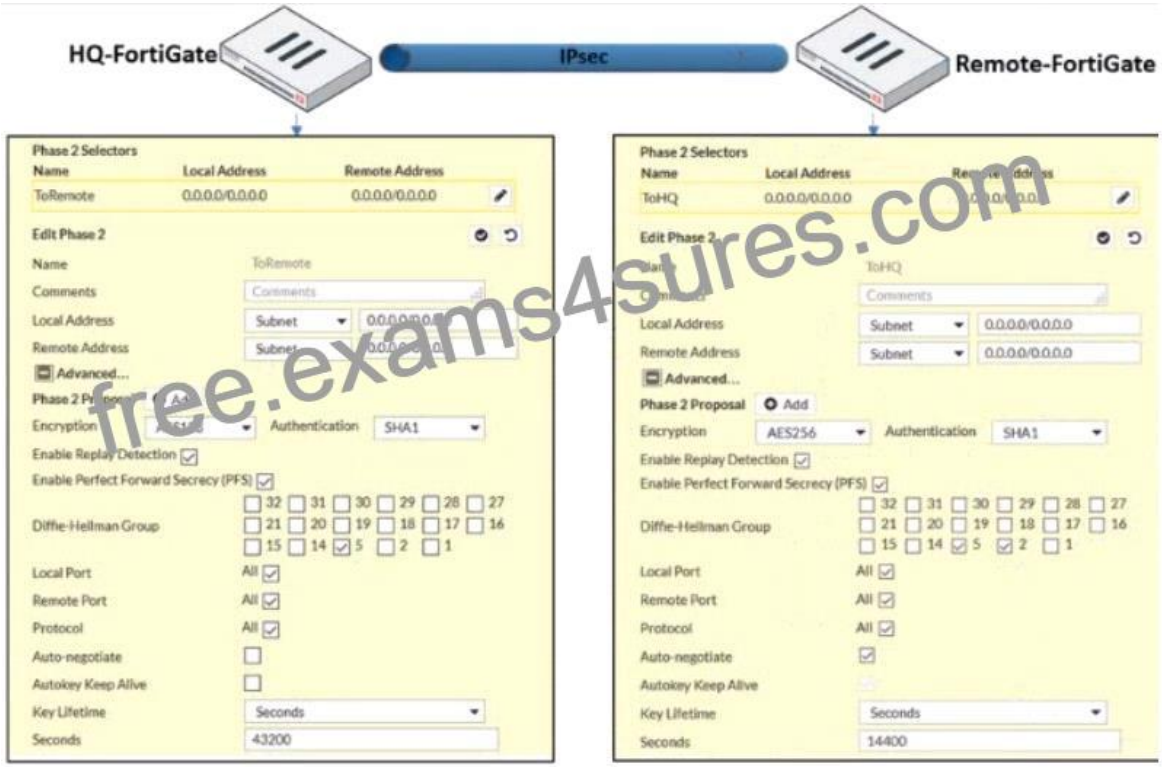
Which Security rating scorecard helps identify configuration weakness and best practice violations in your network?
* Fabric Coverage
* Automated Response
* Security Posture
* Optimization

QUESTION 70

In an explicit proxy setup, where is the authentication method and database configured?
* Proxy Policy
* Authentication Rule
* Firewall Policy
* Authentication scheme

QUESTION 71

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?

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

Reference:

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

QUESTION 72

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

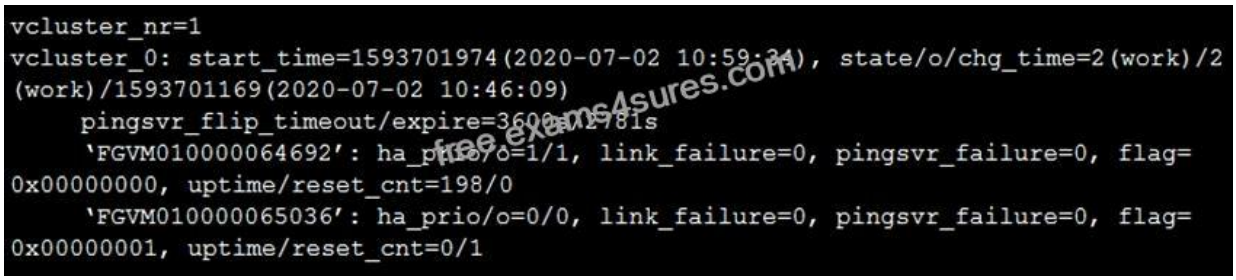
* The collector agent uses a Windows API to query DCs for user logins.
* NetAPI polling can increase bandwidth usage in large networks.
* The collector agent must search security event logs.
* The NetSession Enum function is used to track user logouts.

Reference:

https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD34906&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=210966035&stateId=1%200%20210968009%27)

QUESTION 73

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.)
* FortiGate SN FGVM010000065036 HA uptime has been reset.
* FortiGate devices are not in sync because one device is down.
* FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
* FortiGate SN FGVM010000064692 has the higher HA priority.
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-disabled-default

QUESTION 74

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.

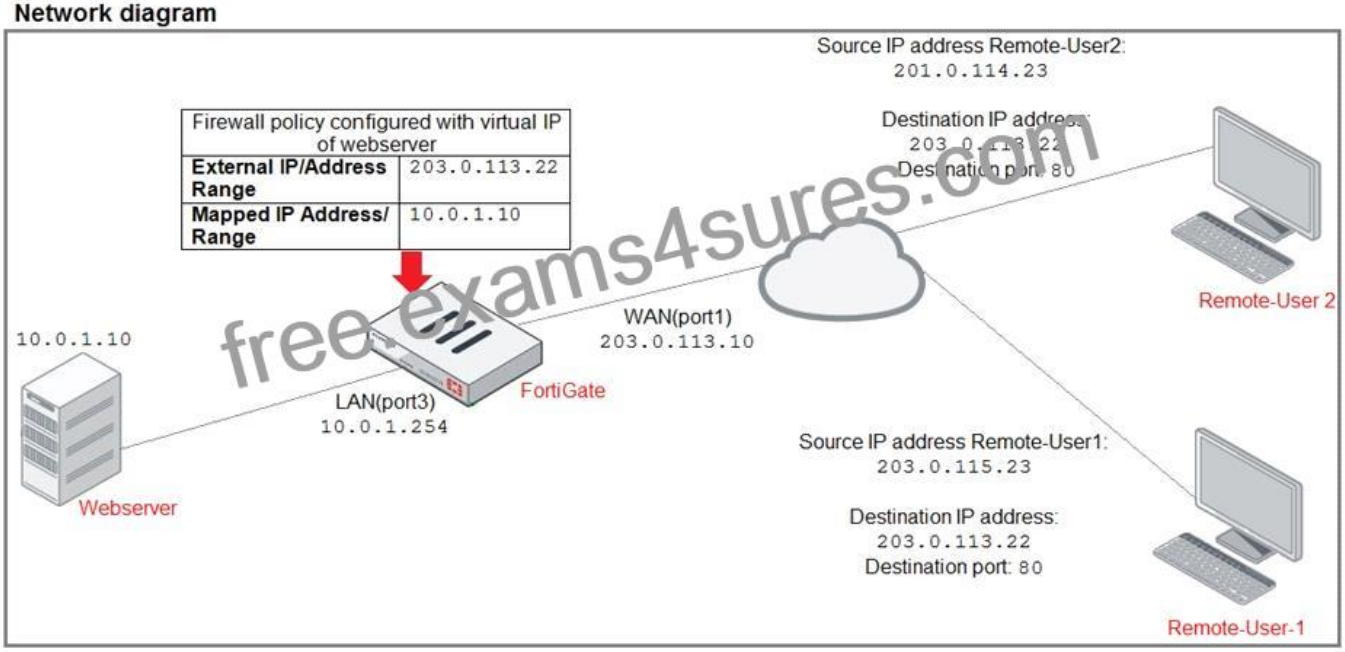
The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.

What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)
* Set the maximum session TTL value for the TELNET service object.
* Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.
* Create a new service object for TELNET and set the maximum session TTL.
* 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.

QUESTION 75

Refer to the exhibit.

Network diagram



ID	Name	Source	Destination	Schedule	Service	Action
WAN(port1) → LAN(port3) 2						
2	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Web_server	always	ALL	ACCEPT

Firewall address object

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.

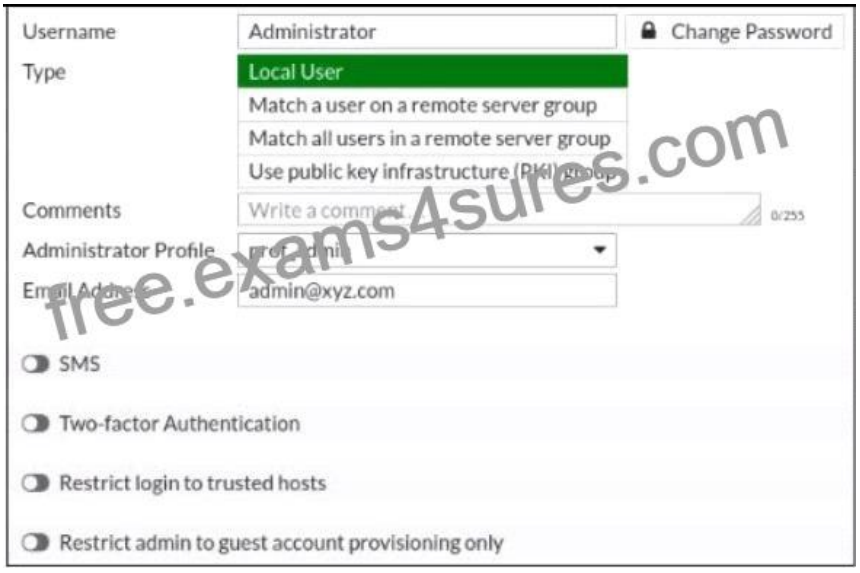
Which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)
* Disable match-vip in the Deny policy.
* Set the Destination address as Deny_IP in the Allow-access policy.
* Enable match vip in the Deny policy.
* Set the Destination address as Web_server in the Deny policy.

QUESTION 76

Which two statements about SSL VPN between two FortiGate devices are true? (Choose two.)
* The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
* The client FortiGate requires a manually added route to remote subnets.
* The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VPN.
* Server FortiGate requires a CA certificate to verify the client FortiGate certificate.

QUESTION 77

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?
* Change password
* Enable restrict access to trusted hosts
* Change Administrator profile
* Enable two-factor authentication

QUESTION 78

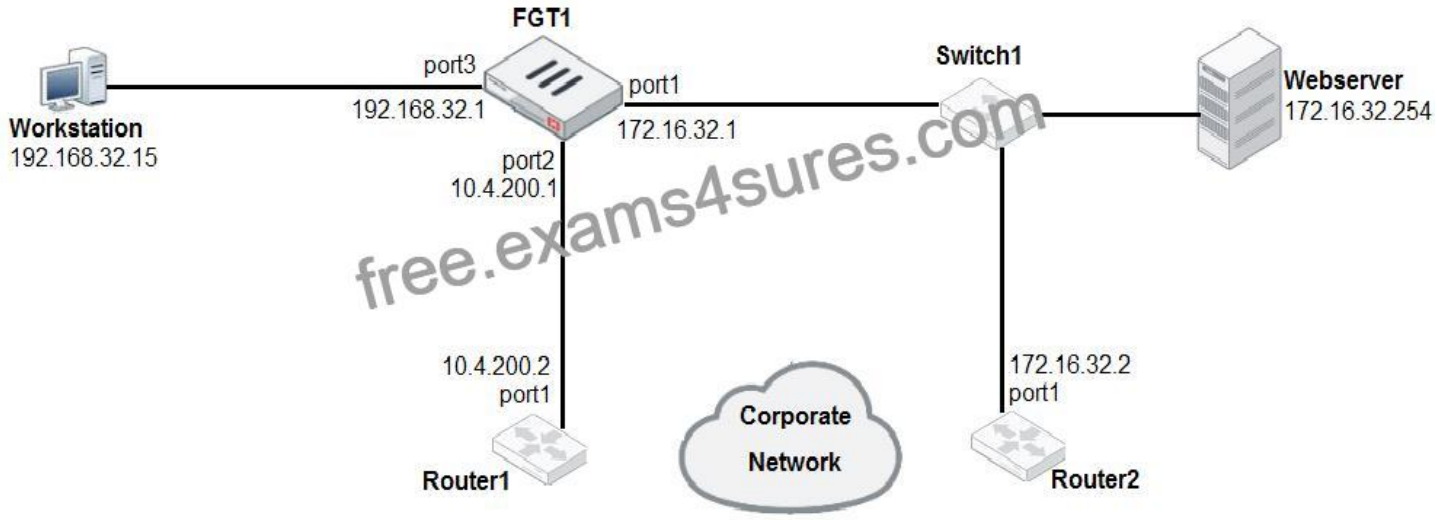
How do you format the FortiGate flash disk?
* Load a debug FortiOS image.
* Load the hardware test (HQIP) image.
* Execute the CLI command execute formatlogdisk.
* Select the format boot device option from the BIOS menu.

QUESTION 79

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?
* 192.168.3.0/24
* 192.168.2.0/24
* 192.168.1.0/24
* 192.168.0.0/8

QUESTION 80

Examine the network diagram shown in the exhibit, then answer the following question:



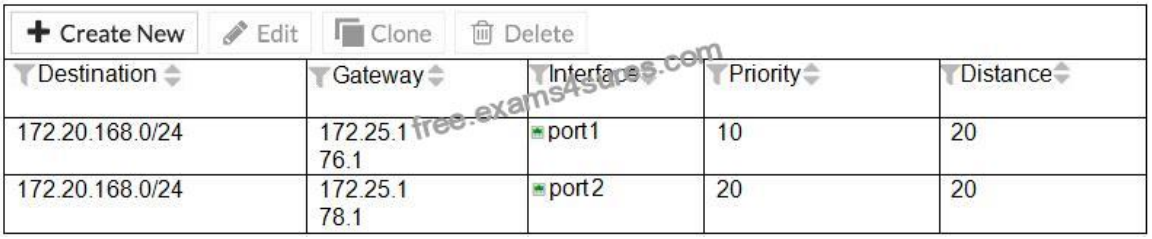
Which one of the following routes is the best candidate route for FGT1 to route traffic from the Workstation to the Web server?
* 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
* 0.0.0.0/0 [20/0] via 10.4.200.2, port2
* 10.4.200.0/30 is directly connected, port2
* 172.16.32.0/24 is directly connected, port1

QUESTION 81

Which two VDOMs are the default VDOMs created when FortiGate is set up in split VDOM mode? (Choose two.)
* FG-traffic
* Mgmt
* FG-Mgmt
* Root

QUESTION 82

Examine the two static routes shown in the exhibit, then answer the following question.



Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?
* FortiGate will load balance all traffic across both routes.
* FortiGate will use the port1 route as the primary candidate.
* FortiGate will route twice as much traffic to the port2 route
* FortiGate will only actuate the port1 route in the routing table
“If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path.”

QUESTION 83

Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)
* Source defined as Internet Services in the firewall policy.
* Destination defined as Internet Services in the firewall policy.
* Highest to lowest priority defined in the firewall policy.
* Services defined in the firewall policy.
* Lowest to highest policy ID number.

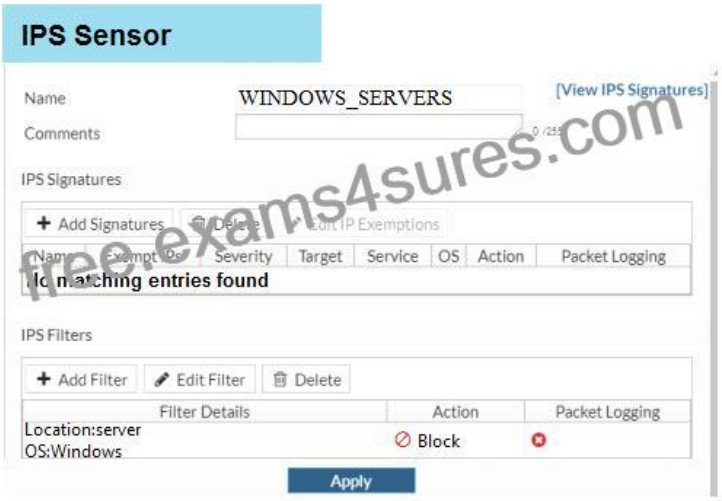
QUESTION 84

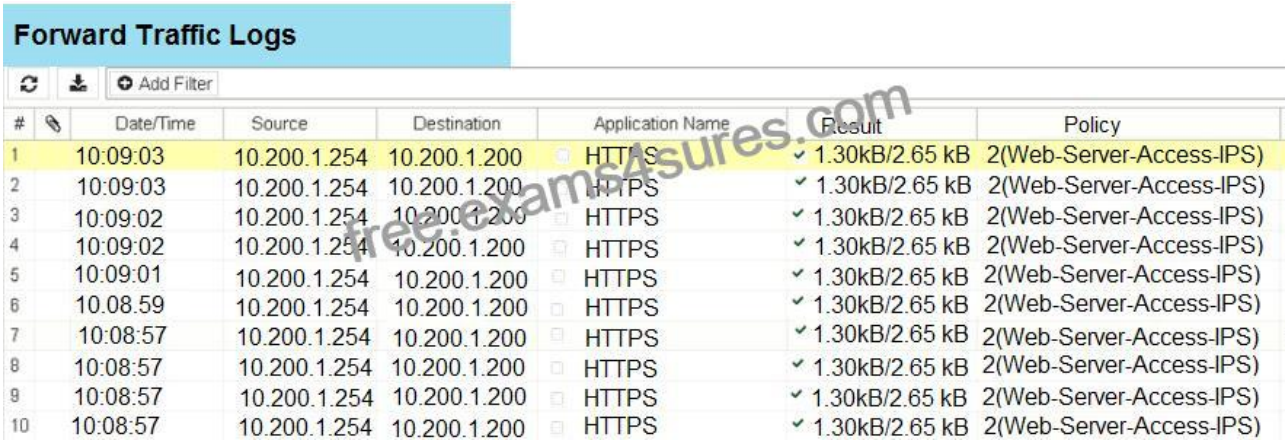
FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.

Which two other security profiles can you apply to the security policy? (Choose two.)
* Antivirus scanning
* File filter
* DNS filter
* Intrusion prevention

QUESTION 85

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?

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

QUESTION 86

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

* FortiManager
* Root FortiGate
* FortiAnalyzer
* Downstream FortiGate

QUESTION 87

Which two statements are true about collector agent standard access mode? (Choose two.)

* Standard mode uses Windows convention-NetBios: DomainUsername.
* Standard mode security profiles apply to organizational units (OU).
* Standard mode security profiles apply to user groups.
* Standard access mode supports nested groups.