

NSE4_FGT-6.4

Number: NSE4_FGT-6.4

Passing Score: 800

Time Limit: 120 min

File Version: 1

NSE4_FGT-6.4



Website: <https://vceplus.com> - <https://vceplus.co>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

<https://vceplus.com/>

Exam A

QUESTION 1

What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?



<https://vceplus.com/>

- A. Full Content inspection
- B. Proxy-based inspection
- C. Certificate inspection
- D. Flow-based inspection

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 2

Which scanning technique on FortiGate can be enabled only on the CLI?

- A. Heuristics scan
- B. Trojan scan
- C. Antivirus scan
- D. Ransomware scan

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/927086/examples>

QUESTION 3

Which two policies must be configured to allow traffic on a policy-based next-generation firewall (NGFW) FortiGate? (Choose two.)

- A. Firewall policy
- B. Policy rule
- C. Security policy
- D. SSL inspection and authentication policy

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/38324/ngfw-policy-based-mode>

QUESTION 4

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%.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 5

Refer to the exhibit, which contains a Performance SLA configuration.

Name	SLA1		
Protocol	Ping	HTTP	DNS
Server	4.2.2.2		✕
	4.2.2.1		✕
Participants	All SD-WAN Members Specify		
	port1		✕
	port2		✕
	+		
Enable probe packets	<input type="checkbox"/>		

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic.

Why is FortiGate not generating any traffic for the performance SLA?

- A. There may not be a static route to route the performance SLA traffic.
- B. You need to turn on the **Enable probe packets** switch.
- C. The Ping protocol is not supported for the public servers that are configured.
- D. Participants configured are not SD-WAN members.

Correct Answer: B

Section: (none)

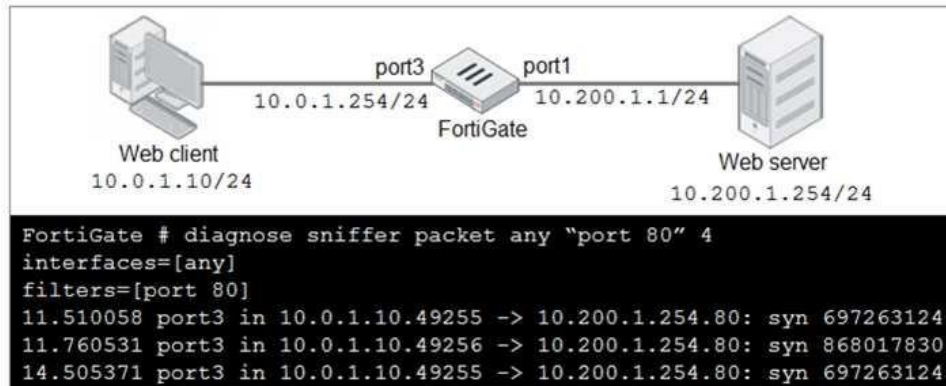
Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/478384/performance-sla-link-monitoring>

QUESTION 6

Refer to the exhibit.



In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.

What should the administrator do next to troubleshoot the problem?

- A. Run a sniffer on the web server.
- B. Capture the traffic using an external sniffer connected to port1.
- C. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10"
- D. Execute a debug flow.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

Refer to the exhibit to view the application control profile.

Edit Application Sensor

Categories

<input checked="" type="checkbox"/> Business (143, 6)	<input checked="" type="checkbox"/> Cloud.IT (47, 1)
<input checked="" type="checkbox"/> Collaboration (255, 10)	<input checked="" type="checkbox"/> Email (78, 12)
<input type="checkbox"/> Game (84)	<input checked="" type="checkbox"/> General.Interest (229, 7)
<input type="checkbox"/> Mobile (3)	<input checked="" type="checkbox"/> Network.Service (330)
<input type="checkbox"/> P2P (56)	<input type="checkbox"/> Proxy (168)
<input type="checkbox"/> Remote.Access (84)	<input type="checkbox"/> Social.Media (116, 31)
<input checked="" type="checkbox"/> Storage.Backup (162, 16)	<input checked="" type="checkbox"/> Update (49)
<input type="checkbox"/> Video/Audio (154, 14)	<input type="checkbox"/> VoIP (24)
<input type="checkbox"/> Web.Client (24)	<input type="checkbox"/> Unknown Applications

☐ Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	<input type="checkbox"/> Block
2	VEND Apple	Filter	<input checked="" type="checkbox"/> Monitor

Users who use Apple FaceTime video conferences are unable to set up meetings.

In this scenario, which statement is true?

- A. Apple FaceTime belongs to the custom monitored filter.
- B. The category of Apple FaceTime is being monitored.
- C. Apple FaceTime belongs to the custom blocked filter.

D. The category of Apple FaceTime is being blocked.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

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

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies>

QUESTION 9

Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin -> sink: org pre->post, reply pre->post dev=5->3/3 ->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53 -> 10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpidb_link_id= 00000000 rpidb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

- A. The session is a UDP unidirectional state.
- B. The session is in TCP `ESTABLISHED` state.
- C. The session is a bidirectional UDP connection.
- D. The session is a bidirectional TCP connection.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

Refer to the exhibit.



Authentication rule

Edit Rule Authentication rule

Name: WebproxyRule

Source Address: LOCAL_SUBNET

Protocol: HTTP

Authentication Scheme: Web-Proxy-Scheme

IP-based Authentication: ☒ Enable ☐ Disable

SSO Authentication Scheme: ☐

Comments: Write a comment... 0/1023

Enable This Rule: ☒ Enable ☐ Disable

Users

[+ Create New](#) [Edit](#) [Delete](#) [Search](#)

Name	Type
User-A	LOCAL
User-B	LOCAL
User-C	LOCAL

Authentication scheme

Edit Authentication Scheme

Name: Web-Proxy-Scheme

Method: Form-based

User database: ☒ Local ☐ Other

Two-factor authentication: ☐

Firewall address

Edit Address

Category: ☒ Address ☐ Proxy Address

Name: LOCAL_SUBNET

Color: Change

Type: Subnet

IP/Netmask: 10.0.1.0/24

Interface: any

Static route configuration: ☐

Comments: Write a comment... 0/255

Proxy address

Edit Address

Category: ☐ Address ☒ Proxy Address

Name: Browser-CAT-1

Color: Change

Type: User Agent

Host: LOCAL_SUBNET

User Agent: Apple Safari

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 10.0.1.10 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.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 11

What devices form the core of the security fabric?

- A. Two FortiGate devices and one FortiManager device
- B. One FortiGate device and one FortiManager device
- C. Two FortiGate devices and one FortiAnalyzer device
- D. One FortiGate device and one FortiAnalyzer device

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/425100/components>

QUESTION 12

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.

Correct Answer: ABD

Section: (none)

Explanation

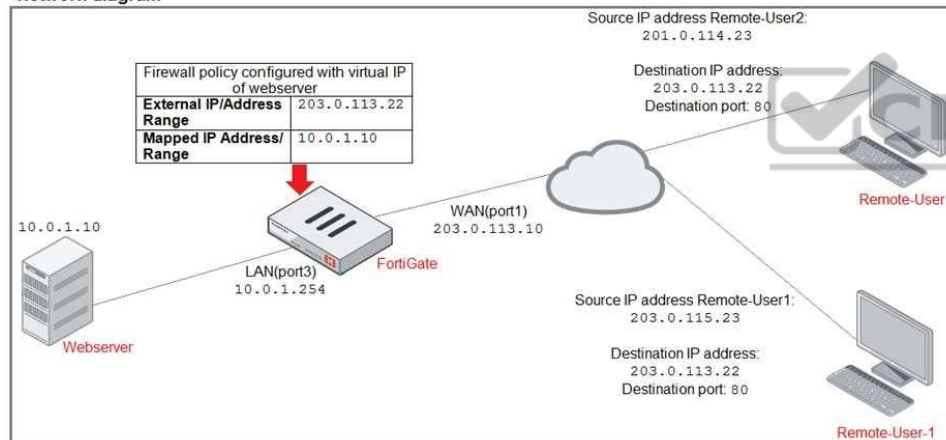
Explanation/Reference:

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

QUESTION 13

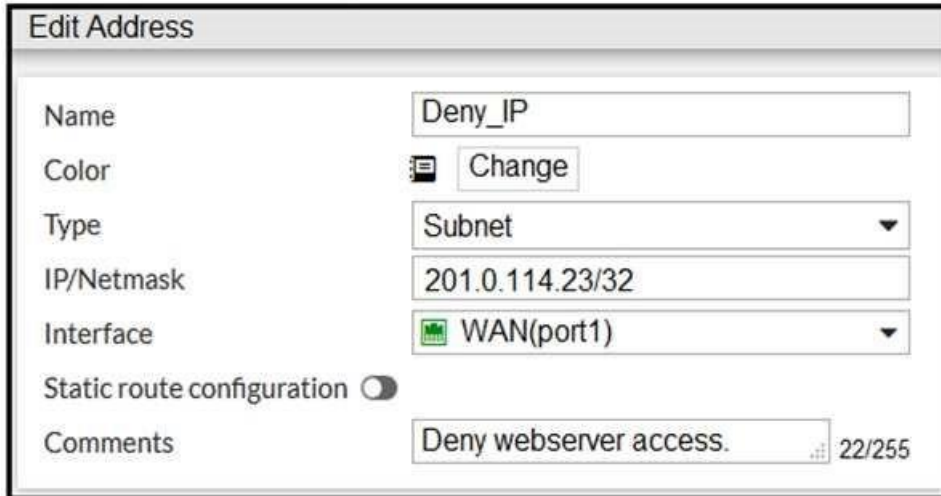
Refer to the exhibit.

Network diagram



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

Firewall address object



Name	Deny_IP
Color	Change
Type	Subnet
IP/Netmask	201.0.114.23/32
Interface	WAN(port1)
Static route configuration	<input type="checkbox"/>
Comments	Deny webserver access. 22/255

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.)

- A. Disable `match-vip` in the **Deny** policy.
- B. Set the **Destination** address as **Deny_IP** in the **Allow-access** policy.
- C. Enable `match vip` in the **Deny** policy.
- D. Set the **Destination** address as **Web_server** in the **Deny** policy.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

- A. SSH
- B. HTTPS
- C. FTM
- D. FortiTelemetry

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/995103/building-security-into-fortios>

QUESTION 15

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.)

- A. Antivirus scanning
- B. File filter
- C. DNS filter
- D. Intrusion prevention



Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Which two types of traffic are managed only by the management VDOM? (Choose two.)

- A. FortiGuard web filter queries
- B. PKI
- C. Traffic shaping
- D. DNS

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

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?

- A. Enable asymmetric routing, so the RPF check will be bypassed.
- B. Disable the RPF check at the FortiGate interface level for the source check.
- C. Disable the RPF check at the FortiGate interface level for the reply check.
- D. Enable asymmetric routing at the interface level.

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955>

QUESTION 18

Refer to the web filter raw logs.

```
date=2020-07-09 time=12:51:51 logid= "0316013057" type= "utm"
subtype= "webfilter" eventtype= "ftgd_blk" level= "warning"
vd= "root" eventtime=1594313511250173744 tz= "-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf= "port2"
srcintfrole= "undefined" dstip=104.244.42.193 dstport=443
dstintf= "port1" dstintfrole= "undefined" proto=6 service= "HTTPS"
hostname= "twitter.com" profile= "all_users_web" action= "blocked"
reqtype= "direct" url= "https://twitter.com/" sentbyte=517
rcvdbyte=0 direction= "outgoing" msg= "URL belongs to a category
with warnings enabled" method= "domain" cat=37 catdesc= "Social
Networking"

date=2020-07-09 time=12:52:16 logid= "0316013057" type= "utm"
subtype= "webfilter" eventtype= "ftgd_blk" level= "warning"
vd= "root" eventtime=1594313537024536428 tz= "-0400" policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf= "port2"
srcintfrole= "undefined" dstip=104.244.42.193 dstport=443
dstintf= "port1" dstintfrole= "undefined" proto=6 service= "HTTPS"
hostname= "twitter.com" profile= "all_users_web"
action= "passthrough" reqtype= "direct" url= "https://twitter.com/"
sentbyte=369 rcvdbyte=0 direction= "outgoing" msg= "URL belongs to
a category with warnings enabled" method= "domain" cat=37
catdesc= "Social Networking"
```

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

- A. Access to the social networking web filter category was explicitly blocked to all users.
- B. The action on firewall policy ID 1 is set to warning.
- C. Social networking web filter category is configured with the action set to authenticate.
- D. The name of the firewall policy is all_users_web.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

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

- A. Standard mode uses Windows convention-NetBios: Domain\Username.
- B. Standard mode security profiles apply to organizational units (OU).
- C. Standard mode security profiles apply to user groups.
- D. Standard access mode supports nested groups.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso>

QUESTION 20

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Exhibit A



Edit Policy

Inspection Mode

Flow-based
Proxy-based

Firewall / Network Options

NAT

☒

IP Pool Configuration

Use Outgoing Interface Address
Use Dynamic IP Pool

Preserve Source Port

☐

Protocol Options

PRX default

Security Profiles

AntiVirus

☒

AV default

Web Filter

☐

DNS Filter

☐

Application Control

☐

IPS

☐

SSL Inspection

☒

SSL deep-inspection

Decrypted Traffic Mirror

☐

Exhibit B

Edit AntiVirus Profile

Name:

Comments: 29/255

Detect Viruses: **Block** Monitor

Feature set: **Flow-based** Proxy-based

Inspected Protocols

HTTP ☒

SMTP ☒

POP3 ☒

IMAP ☒

FTP ☒

CIFS ☐

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ☒

Include Mobile Malware Protection ☒

Virus Outbreak Prevention ⓘ

Use FortiGuard Outbreak Prevention Database ☐

Use External Malware Block List ⓘ ⚠ ☐

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The volume of traffic being inspected is too high for this model of FortiGate.
- B. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.
- C. The firewall policy performs the full content inspection on the file.
- D. The flow-based inspection is used, which resets the last packet to the user.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

Which three methods are used by the collector agent for AD polling? (Choose three.)

- A. FortiGate polling
- B. NetAPI
- C. Novell API
- D. WMI
- E. WinSecLog

Correct Answer: BDE

Section: (none)

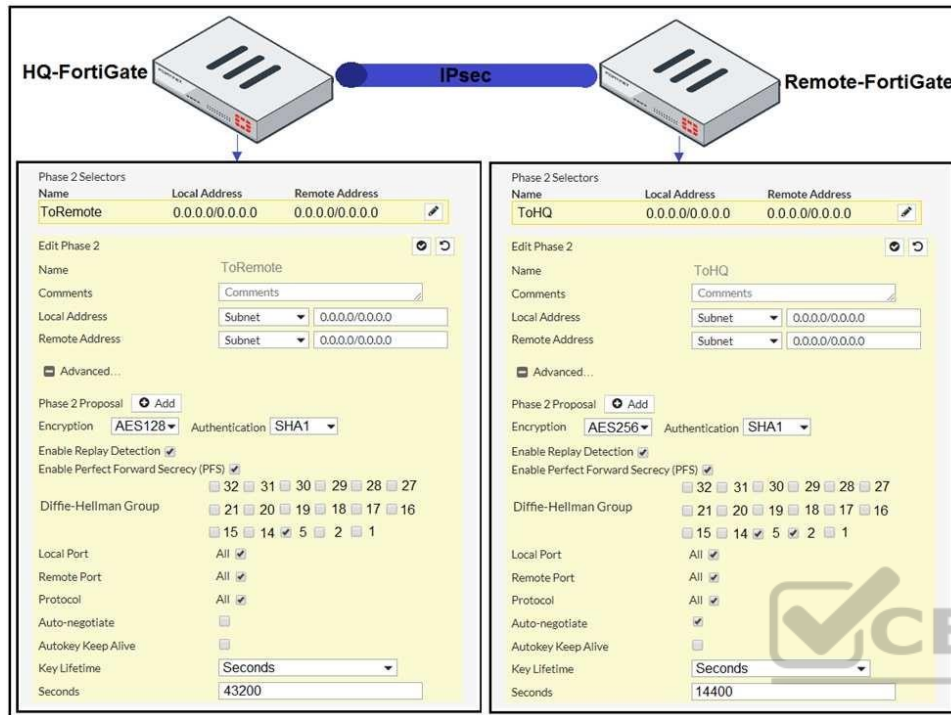
Explanation

Explanation/Reference:

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

QUESTION 22

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/168495>

QUESTION 23

What is the primary FortiGate election process when the HA override setting is disabled?

- A. Connected monitored ports > System uptime > Priority > FortiGate Serial number
- B. Connected monitored ports > HA uptime > Priority > FortiGate Serial number
- C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number
- D. Connected monitored ports > Priority > System uptime > FortiGate Serial number

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <http://myitmicroblog.blogspot.com/2018/11/what-should-you-know-about-ha-override.html>

QUESTION 24

Refer to the exhibit, which contains a static route configuration.



Edit Static Route

Destination ⓘ Subnet Internet Service
 Amazon-AWS

Gateway Address 10.200.1.254

Interface port1

Comments Write a comment... 0/255

Status Enabled Disabled

An administrator created a static route for Amazon Web Services.

What CLI command must the administrator use to view the route?

- A. `get router info routing-table all`

- B. get internet service route list
- C. get router info routing-table database
- D. diagnose firewall proute list

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.fortinetguru.com/2019/09/troubleshooting-sd-wan-fortios-6-2/>

QUESTION 25

Refer to the exhibit.

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg= "vd-root received a
packet(proto=1, 10.0.1.10:1-> 10.200.1.254:2048) from port3. type=8, code=0
id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg= "allocate a
new session-00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg= "find a
route: flag=04000000 gw=10.200.1.254 via port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg= "Denied by forward
policy check (policy 0)"
```

Why did FortiGate drop the packet?

- A. It matched an explicitly configured firewall policy with the action **DENY**.
- B. The next-hop IP address is unreachable.
- C. It failed the RPF check.
- D. It matched the default implicit firewall policy.

Correct Answer: D

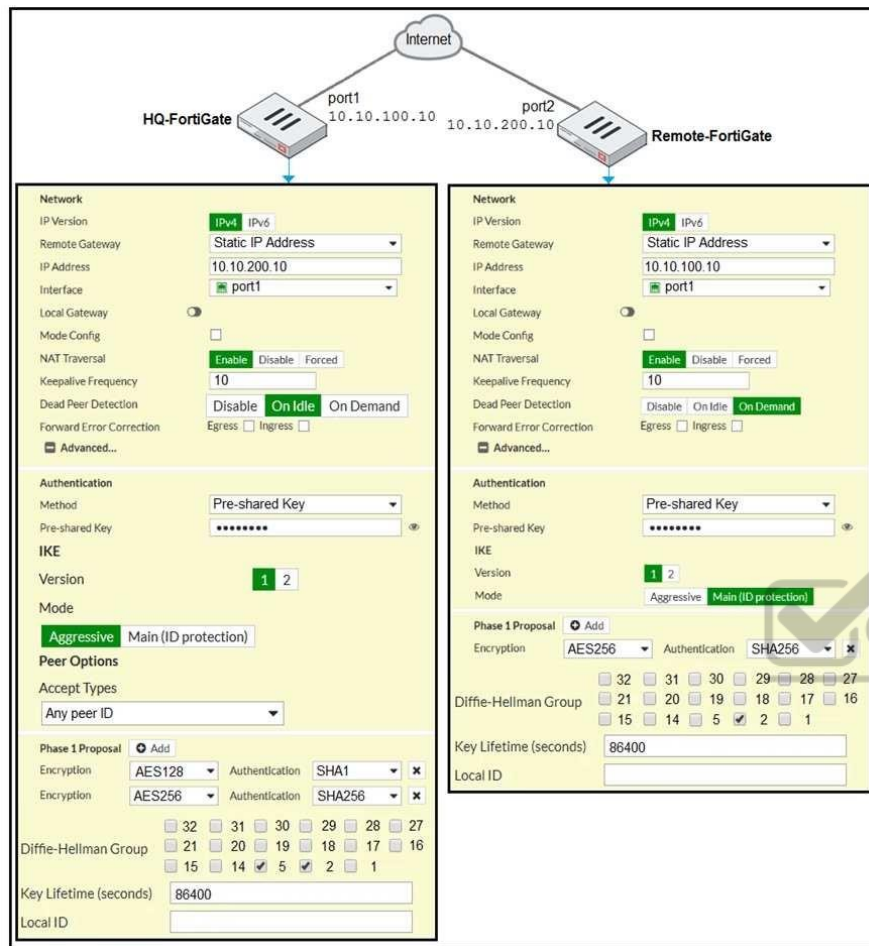
Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.

Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

- A. On HQ-FortiGate, set IKE mode to **Main (ID protection)**.
- B. On both FortiGate devices, set **Dead Peer Detection** to **On Demand**.

- C. On HQ-FortiGate, disable **Diffie-Helman group 2**.
- D. On Remote-FortiGate, set **port2** as **Interface**.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

Which two statements are true about the RPF check? (Choose two.)

- A. The RPF check is run on the first sent packet of any new session.
- B. The RPF check is run on the first reply packet of any new session.
- C. The RPF check is run on the first sent and reply packet of any new session.
- D. RPF is a mechanism that protects FortiGuard and your network from IP spoofing attacks.

Correct Answer: AD

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://www.programmersought.com/article/16383871634/>

QUESTION 28

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/758820/split-task-vdom-mode>

QUESTION 30

Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

- A. `diagnose sys top`
- B. `execute ping`
- C. `execute traceroute`
- D. `diagnose sniffer packet any`
- E. `get system arp`



Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>

