

NSE4_FGT-6.4.VCEplus.premium.exam.60q

Number: NSE4_FGT-6.4
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Website: <https://vceplus.com>

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

NSE4_FGT-6.4

Fortinet NSE 4 - FortiOS 6.4



Exam A

QUESTION 1 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

Section: (none)

Explanation

Explanation/Reference:

Reference: [https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate Transparent Mode Technical Guide FortiOS 4 0 version1.2.pdf&documentID=FD33113](https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate%20Transparent%20Mode%20Technical%20Guide%20FortiOS%204.0%20version1.2.pdf&documentID=FD33113)

QUESTION 2

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 3

Which two statements about IPsec authentication on FortiGate are correct? (Choose two.)

- A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password
- B. FortiGate supports pre-shared key and signature as authentication methods.
- C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.
- D. A certificate is not required on the remote peer when you set the signature as the authentication method.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/913287/ipsec-vpn-authenticating-a-remote-fortigate-peer-with-a-pre-shared-key>

QUESTION 4

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: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/567568/enabling-scanning>

QUESTION 5 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 6

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)

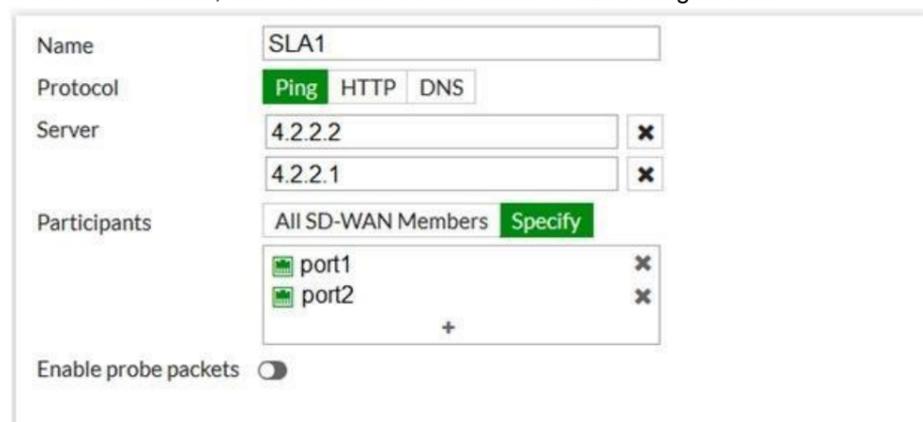
Explanation

Explanation/Reference:

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

QUESTION 7

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



The screenshot shows the configuration for a Performance SLA named 'SLA1'. The 'Protocol' is set to 'Ping'. The 'Server' field contains two IP addresses: '4.2.2.2' and '4.2.2.1'. The 'Participants' field is set to 'All SD-WAN Members'. Below this, there are two port entries: 'port1' and 'port2'. At the bottom, there is a toggle for 'Enable probe packets' which is currently turned off.

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: D

Section: (none)

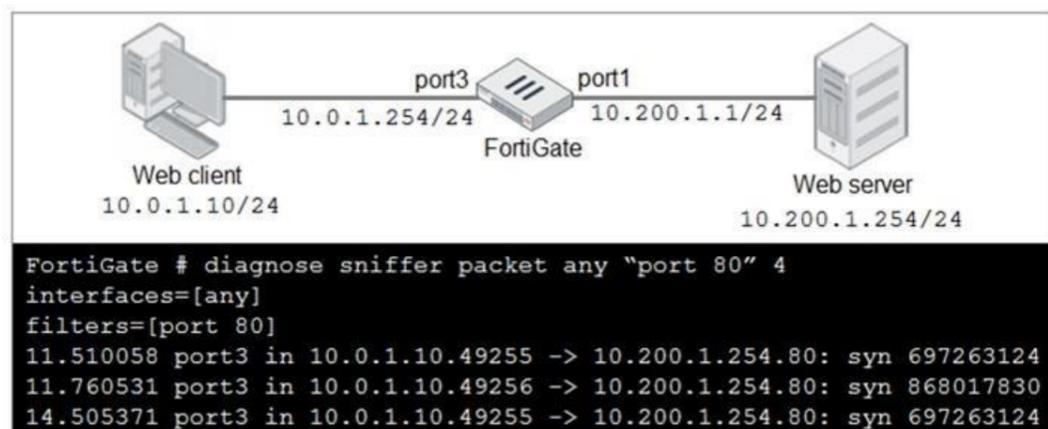
Explanation

Explanation/Reference:

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

QUESTION 8

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 9

Refer to the exhibit to view the application control profile.

Edit Application Sensor

Categories

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

Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	<input type="button" value="Block"/>
2	VEND Apple	Filter	<input type="button" value="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 10 What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

- A. FortiGate automatically negotiates different local and remote addresses with the remote peer.
- B. FortiGate automatically negotiates a new security association after the existing security association expires.
- C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
- D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=12069>

QUESTION 11 Which three security features require the intrusion prevention system (IPS) engine to function?
(Choose three.)

- A. Web filter in flow-based inspection
- B. Antivirus in flow-based inspection
- C. DNS filter
- D. Web application firewall
- E. Application control

Correct Answer: ACE

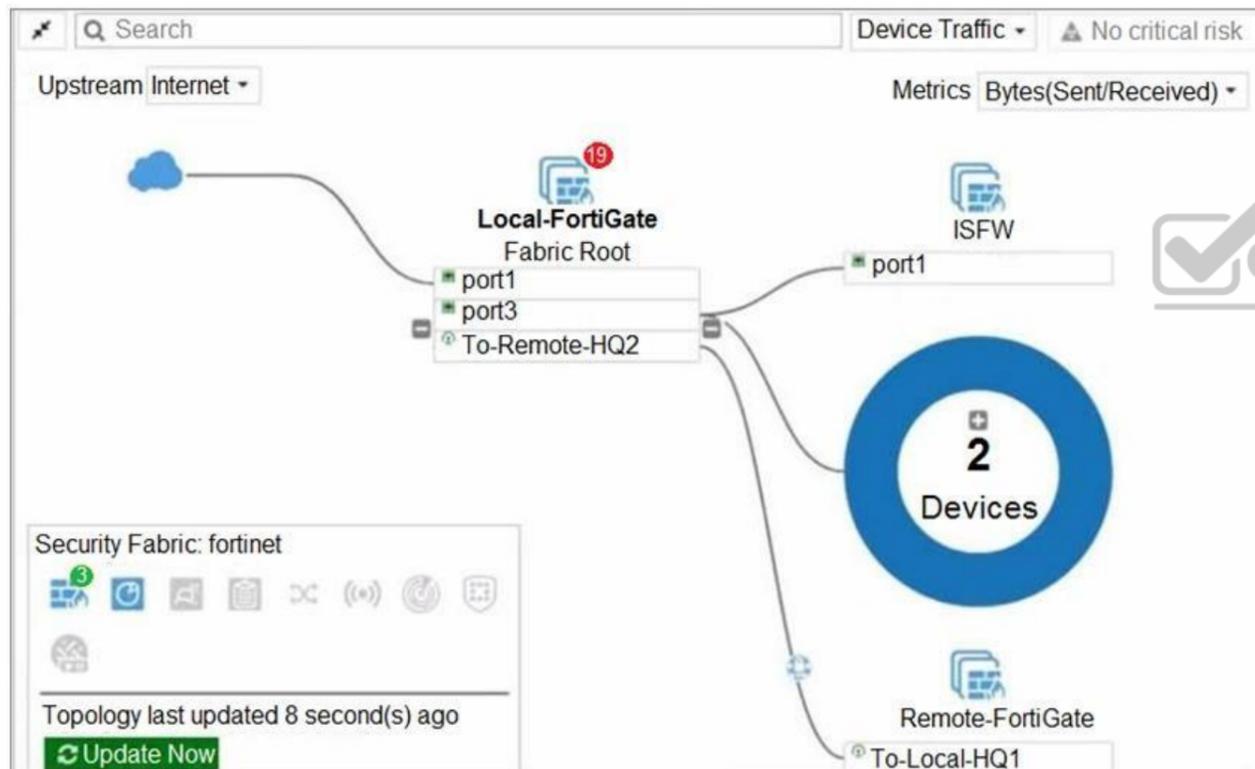
Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Refer to the exhibit.



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

- A. There are five devices that are part of the security fabric.
- B. Device detection is disabled on all FortiGate devices.
- C. This security fabric topology is a logical topology view.
- D. There are 19 security recommendations for the security fabric.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile.

What order must FortiGate use when the web filter profile has features enabled, such as safe search?

- A. DNS-based web filter and proxy-based web filter
- B. Static URL filter, FortiGuard category filter, and advanced filters
- C. Static domain filter, SSL inspection filter, and external connectors filters
- D. FortiGuard category filter and rating filter

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: https://fortinet121.rssing.com/chan-67705148/all_p1.html

QUESTION 14 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 15

Refer to the exhibit to view the firewall policy.

Name 	Internet Access
Incoming Interface	 port2
Outgoing Interface	 port1
Source	 all ✕
	+
Destination	 all ✕
	+
Schedule	 always
Service	<input checked="" type="checkbox"/> DNS ✕ <input checked="" type="checkbox"/> FTP ✕ <input checked="" type="checkbox"/> HTTP ✕ <input checked="" type="checkbox"/> HTTPS ✕ <div style="text-align: center;">+</div>
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based
Security Profiles	
AntiVirus	<input checked="" type="checkbox"/> AV default ✎
Web Filter	<input type="checkbox"/>
DNS Filter	<input type="checkbox"/>
Application Control	<input type="checkbox"/>
IPS	<input type="checkbox"/>



Which statement is correct if well-known viruses are not being blocked?

- A. The firewall policy does not apply deep content inspection.
- B. The firewall policy must be configured in proxy-based inspection mode.
- C. The action on the firewall policy must be set to deny.
- D. Web filter should be enabled on the firewall policy to complement the antivirus profile.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

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
rpdb_link_id= 00000000 rpdb_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: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 17

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, Google Chrome, Microsoft Internet Explorer or Spart

Comments: Write a comment... 0/255

Proxy address

Edit Address

Category: Address | Proxy Address

Name: Browser-CAT-2

Color: Change

Type: User Agent

Host: LOCAL_SUBNET

User Agent: Mozilla Firefox

Comments: Write a comment... 0/255

Web proxy address

ID	Source	Destination	Schedule	Action
explicit-web proxy → port1				
1	Browser-CAT-2 LOCAL_SUBNET User-B	all	always	DENY
2	LOCAL_SUBNET Browser-CAT-1	all	always	ACCEPT



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: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

Refer to the exhibit.

Exhibit A

Interfaces	Gateway	Cost
port1	100.64.1.254	15
port2	100.64.2.254	5
port3	100.64.3.254	5
port4	100.64.4.254	1

SD-WAN Member

Performance SLA

Name: SLA_1

Protocol: Ping HTTP DNS

Server: 4.2.2.2
4.2.2.1

Participants: All SD-WAN Members

port1
 port2
 port3
 port4

Enable probe packets:

SLA Target

Latency threshold: 50 ms

Jitter threshold: 5 ms

Packet Loss threshold: 0 %

SD-WAN Rule

Outgoing Interfaces

- Manual**
Manually assign outgoing interfaces.
- Best Quality**
The interface with the best measured performance is selected.
- Lowest Cost (SLA)**
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.
- Maximize Bandwidth (SLA)**
Traffic is load balanced among interfaces that meet SLA targets.

Interface preference:
 port4
 port3
 port2
 port1

Required SLA target: SLA_1

Status:



Exhibit B

```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(SLA_1):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x1
Seq(2 port2): state(alive), packet-loss(0.000%) latency(34.349), jitter(3.887) sla_map=0x1
Seq(3 port3): state(alive), packet-loss(0.000%) latency(31.476), jitter(3.254) sla_map=0x1
Seq(4 port4): state(alive), packet-loss(2.130%) latency(46.229), jitter(4.287) sla_map=0x1
```

The exhibit shows the configuration for the SD-WAN member, Performance SLA and SD-WAN Rule, as well as the output of `diagnose sys virtual wan link health-check`.

Which interface will be selected as an outgoing interface?

- A. port4
- B. port2
- C. port1
- D. port3

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19 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 20 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 21 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22 Which security feature does FortiGate provide to protect servers located in the internal networks from attacks such as SQL injections?

- A. Denial of Service
- B. Web application firewall
- C. Antivirus
- D. Application control

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortiweb/6.3.3/administration-guide/60895/introduction>

QUESTION 23

Refer to the exhibit.



Add Signatures

Type: Filter **Signature**

Action: Block

Packet logging: Enable Disable

Status: Enable Disable Default

Rate-based settings: **Default** Specify

Exempt IPs: 0

Search Selected 1 All

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 1					
FTP.Login.Failed	<div style="width: 10px; height: 10px; background-color: green; border: 1px solid gray;"></div>	Server	All	<input checked="" type="checkbox"/> Pass	

Review the Intrusion Prevention System (IPS) profile signature settings.

Which statement is correct in adding the **FTP.Login.Failed** signature to the IPS sensor profile?

- A. Traffic matching the signature will be silently dropped and logged.
- B. The signature setting uses a custom rating threshold.
- C. The signature setting includes a group of other signatures.
- D. Traffic matching the signature will be allowed and logged.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

How does FortiGate act when using SSL VPN in web mode?

- A. FortiGate acts as an FDS server.
- B. FortiGate acts as an HTTP reverse proxy.
- C. FortiGate acts as DNS server.
- D. FortiGate acts as router.

Correct Answer: C

Section: (none)

Explanation

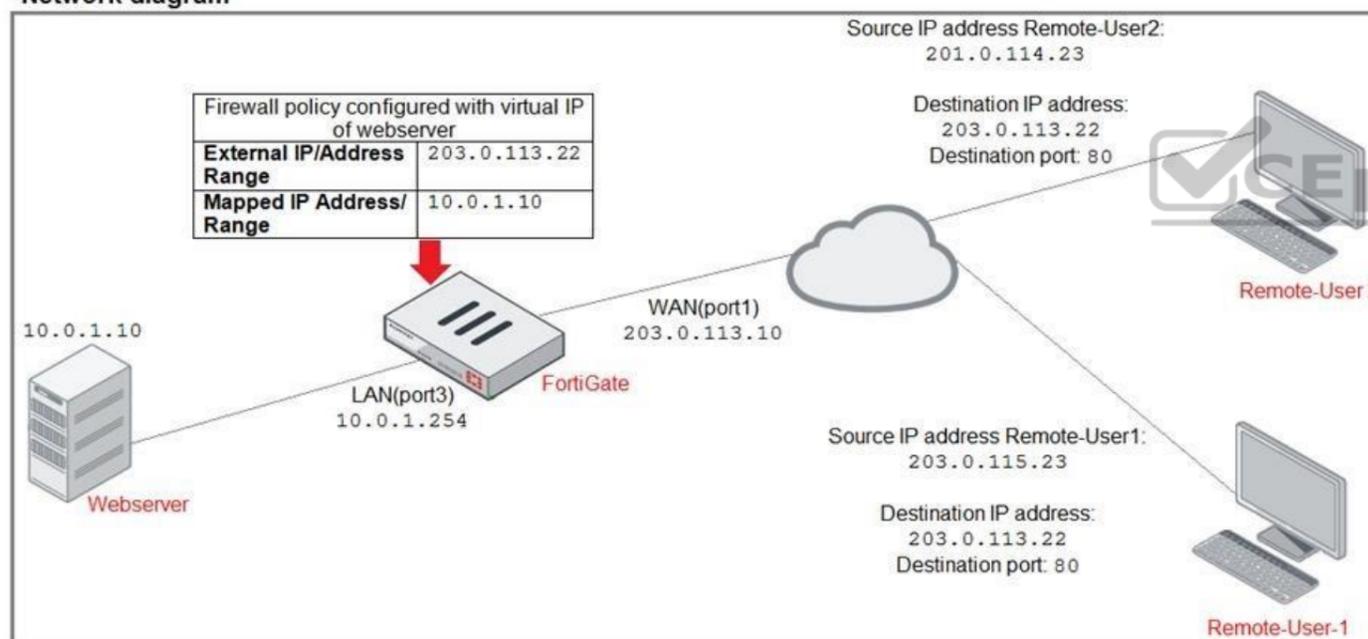
Explanation/Reference:

Reference: https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigate-sslvpn-40-mr3.pdf

QUESTION 25

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

Edit Address

Name	<input type="text" value="Deny_IP"/>
Color	<input type="button" value="Change"/>
Type	<input style="border: none; background-color: #f0f0f0;" type="text" value="Subnet"/>
IP/Netmask	<input type="text" value="201.0.114.23/32"/>
Interface	<input type="text" value="WAN(port1)"/>
Static route configuration	<input type="checkbox"/>
Comments	<input style="width: 90%;" type="text" value="Deny webservice 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: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

- A. The subject field in the server certificate
- B. The serial number in the server certificate
- C. The server name indication (SNI) extension in the client hello message
- D. The subject alternative name (SAN) field in the server certificate
- E. The host field in the HTTP header

Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://checkthefirewall.com/blogs/fortinet/ssl-inspection>

QUESTION 27 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 28

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale      : english

Service    : Web-Filter
Status     : Enable
License    : Contract

Num. of servers : 1
Protocol    : https
Port       : 443
Anycast    : Enable
Default servers : Not included
-- Server List (Tue Feb 1 12:00:25 2020) --

IP           Weight   RTT  Flags  TZ      Packets  Curr Lost  Total Lost
173.243.138.210  10      85  DI     -8      868      0          0
96.45.33.68    10      270 -8      -8      868      0          0
173.243.138.211  10      340 -8      -8      859      0          0
```

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

- 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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29

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 30 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: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31 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 32 A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

- All traffic must be routed through the primary tunnel when both tunnels are up.
- The secondary tunnel must be used only if the primary tunnel goes down.
- In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover.

Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two.)

- A. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
- B. Enable **Dead Peer Detection**.
- C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
- D. Enable **Auto-negotiate** and **Autokey Keep Alive** on the phase 2 configuration of both tunnels.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

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-vlan1	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.)

- A. Traffic between port2 and port2-vlan1 is allowed by default.
- B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
- C. port1 is a native VLAN.
- D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.



Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34 Which two statements are correct about SLA targets? (Choose two.)

- A. You can configure only two SLA targets per one Performance SLA.
- B. SLA targets are optional.
- C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
- D. SLA targets are used only when referenced by an SD-WAN rule.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

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
rcvbyte=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 rcvbyte=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 36 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 37 Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Exhibit A



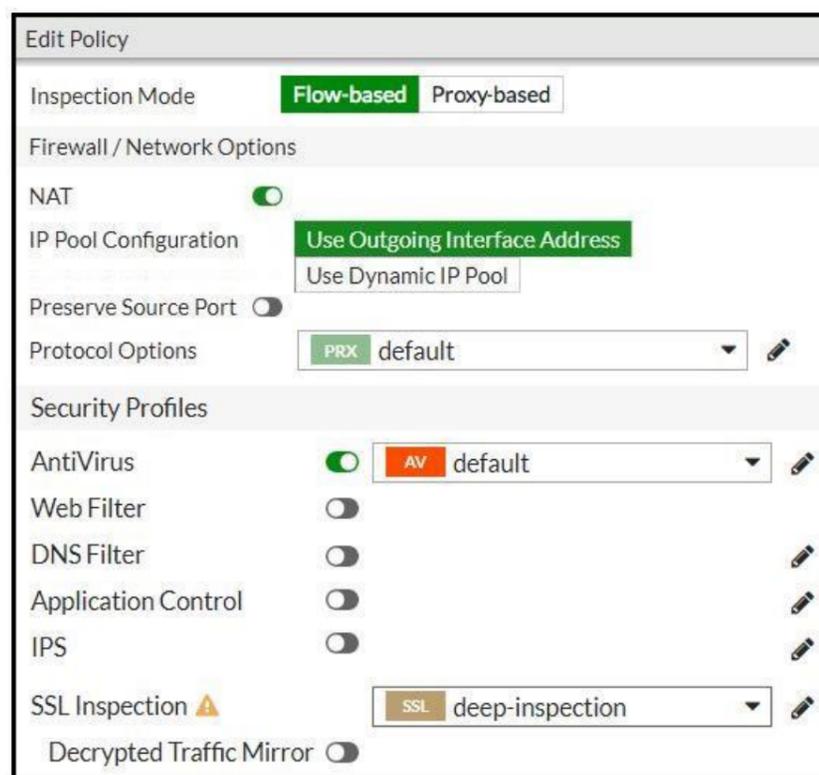


Exhibit B

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 38

Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srcintfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" reqtype= "direct" url= "https://etp-experiment-1.dummytracker.org/"
sentbyte=517 rcvbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

Based on the raw log, which two statements are correct? (Choose two.)

- A. Traffic is blocked because **Action** is set to **DENY** in the firewall policy.
- B. Traffic belongs to the root VDOM.
- C. This is a security log.
- D. Log severity is set to `error` on FortiGate.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39 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

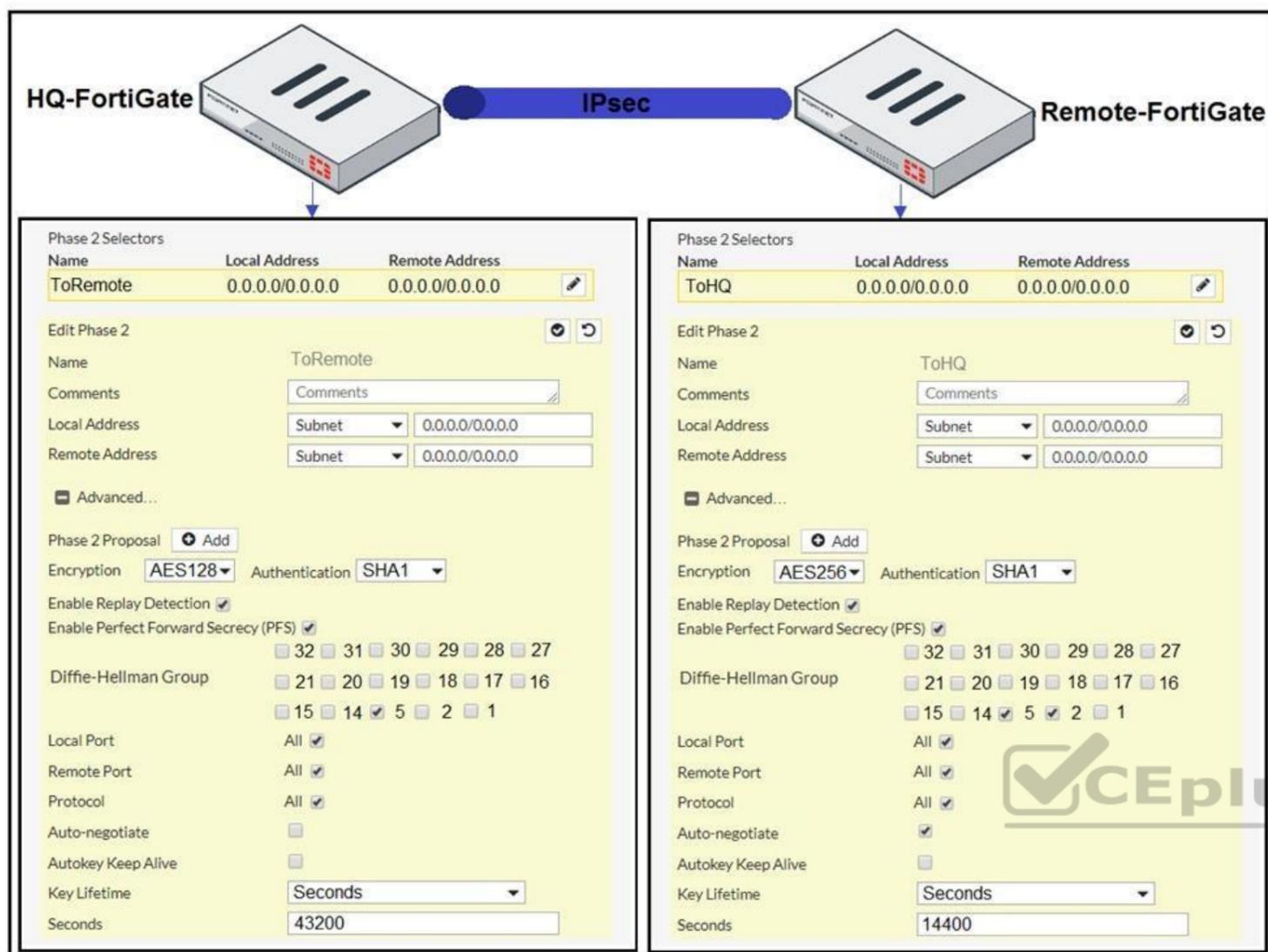
Explanation/Reference:

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

QUESTION 40

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 41

If **Internet Service** is already selected as **Source** in a firewall policy, which other configuration objects can be added to the **Source** field 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: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 42

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.)

A. Set the maximum session TTL value for the TELNET service object.

B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.

C. Create a new service object for TELNET and set the maximum session TTL.

D. 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.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 43

Which Security rating scorecard helps identify configuration weakness and best practice violations in your network?

A. Fabric Coverage

B. Automated Response

C. Security Posture

D. Optimization

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.fortinet.com/content/dam/fortinet/assets/support/fortinet-recommended-security-best-practices.pdf>

QUESTION 44 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

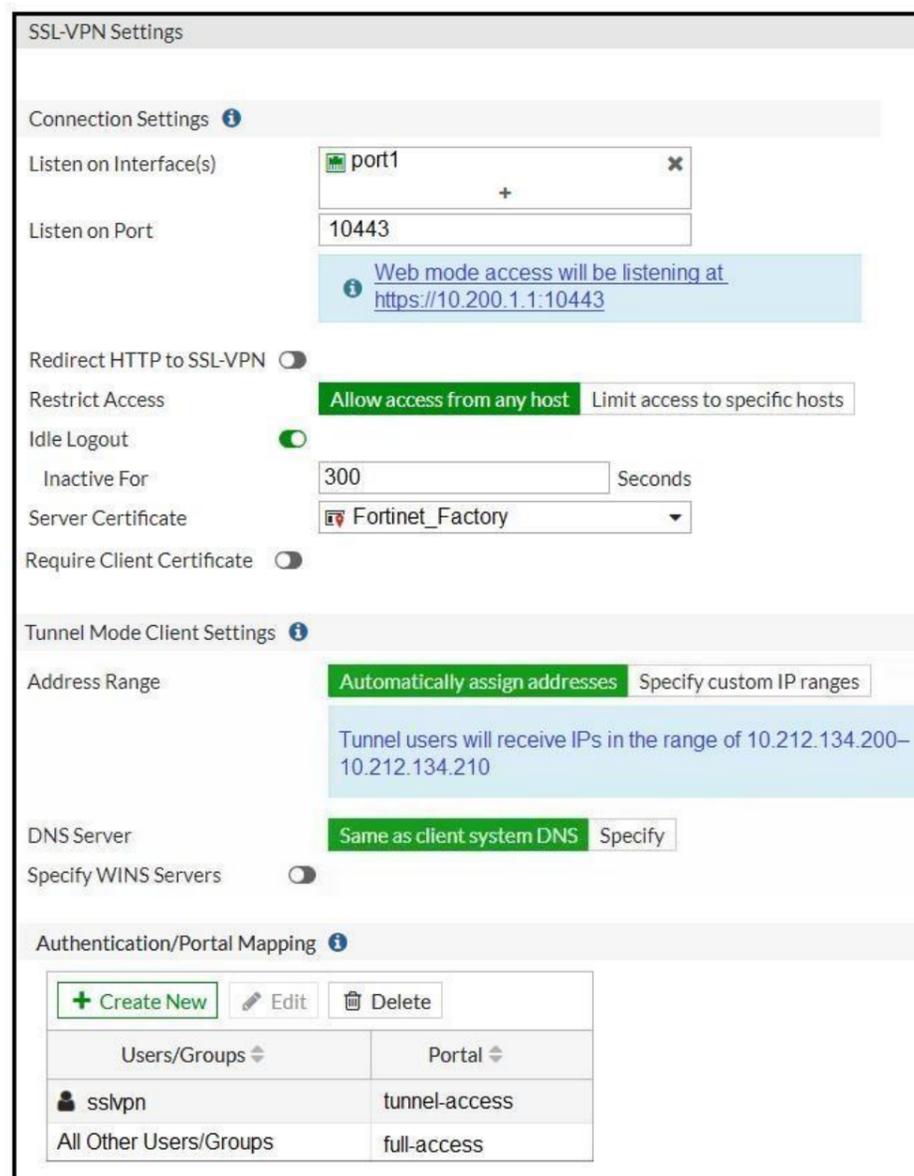
Explanation/Reference:

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

QUESTION 45

Refer to the exhibit.

Exhibit A



The screenshot shows the SSL-VPN Settings configuration page. It is divided into three main sections: Connection Settings, Tunnel Mode Client Settings, and Authentication/Portal Mapping.

Connection Settings:

- Listen on Interface(s): port1
- Listen on Port: 10443
- Web mode access will be listening at <https://10.200.1.1:10443>
- Redirect HTTP to SSL-VPN:
- Restrict Access: **Allow access from any host** (selected), Limit access to specific hosts
- Idle Logout:
- Inactive For: 300 Seconds
- Server Certificate: Fortinet_Factory
- Require Client Certificate:

Tunnel Mode Client Settings:

- Address Range: **Automatically assign addresses** (selected), Specify custom IP ranges
- Tunnel users will receive IPs in the range of 10.212.134.200–10.212.134.210
- DNS Server: **Same as client system DNS** (selected), Specify
- Specify WINS Servers:

Authentication/Portal Mapping:

Buttons: + Create New, Edit, Delete

Users/Groups	Portal
sslvpn	tunnel-access
All Other Users/Groups	full-access



Exhibit B



The SSL VPN connection fails when a user attempts to connect to it.

What should the user do to successfully connect to SSL VPN?

- A. Change the SSL VPN port on the client.
- B. Change the Server IP address.
- C. Change the `idle-timeout`.
- D. Change the SSL VPN portal to the tunnel.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/150494>



QUESTION 46 Which three statements are true regarding session-based authentication?
(Choose three.)

- A. HTTP sessions are treated as a single user.
- B. IP sessions from the same source IP address are treated as a single user.
- C. It can differentiate among multiple clients behind the same source IP address.
- D. It requires more resources.
- E. It is not recommended if multiple users are behind the source NAT

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

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

Edit Static Route

Destination ⓘ Subnet Internet Service

G Amazon-AWS ▼

Gateway Address

Interface port1 ▼

Comments 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: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/latest/administration-guide/139692/routing-concepts>



QUESTION 48 An administrator needs to increase network bandwidth and provide redundancy.

What interface type must the administrator select to bind multiple FortiGate interfaces?

- A. VLAN interface
- B. Software Switch interface
- C. Aggregate interface
- D. Redundant interface

Correct Answer: B

Section: (none)

Explanation

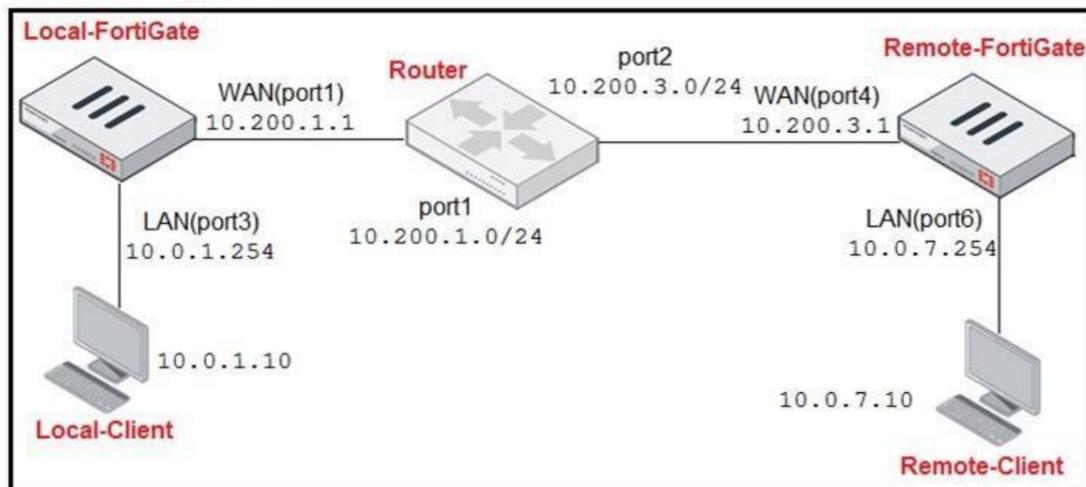
Explanation/Reference:

Reference: <https://forum.fortinet.com/tm.aspx?m=120324>

QUESTION 49

Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

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

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	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)?

- A. 10.200.1.149
- B. 10.200.1.1
- C. 10.200.1.49
- D. 10.200.1.99

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway.

What must an administrator do to achieve this objective?

- A. The administrator can register the same FortiToken on more than one FortiGate.
- B. The administrator must use a FortiAuthenticator device.
- C. The administrator can use a third-party radius OTP server.
- D. The administrator must use the user self-registration server.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 51

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: B

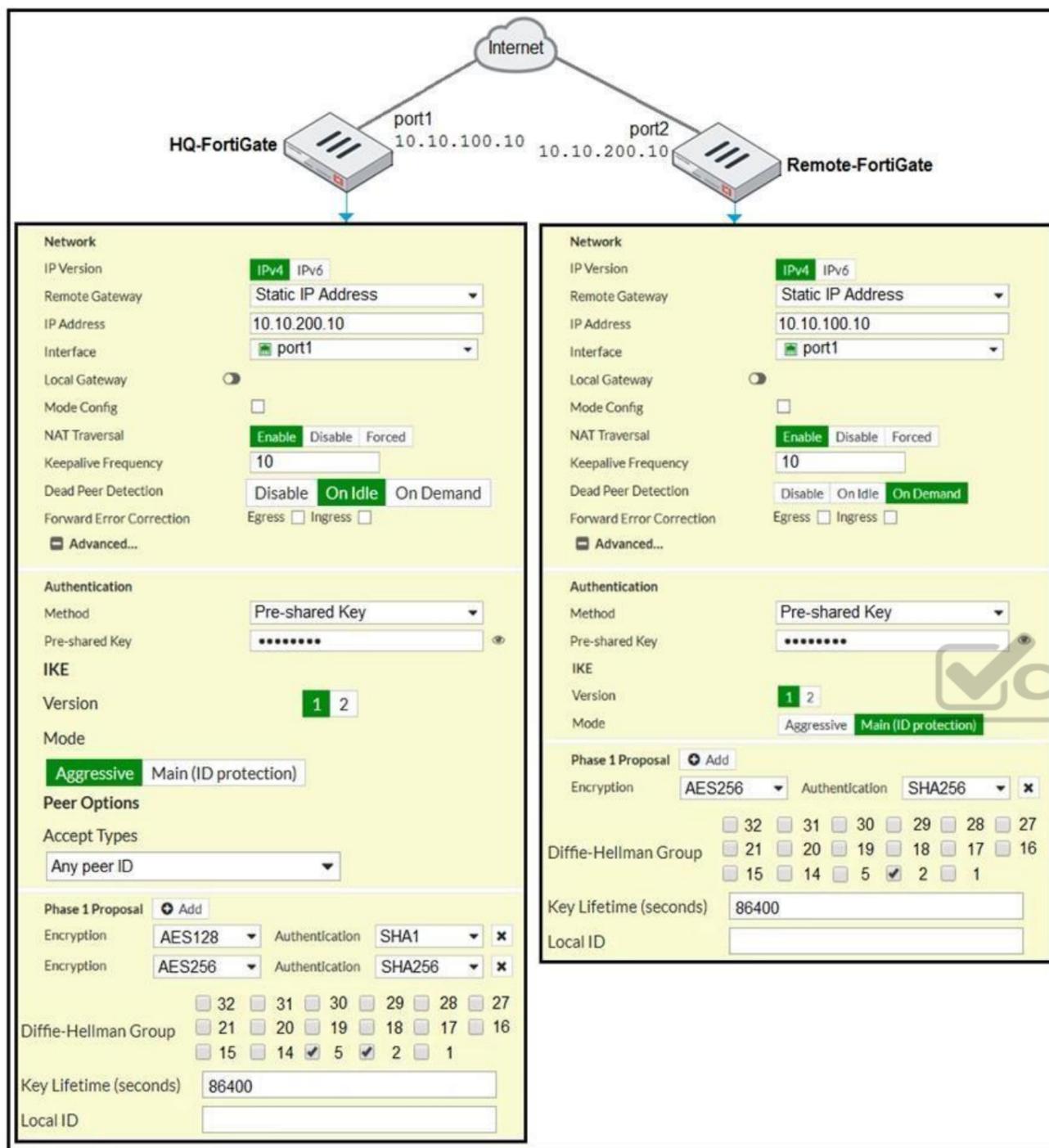
Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

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 53 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?

- A. Change the `session-ttl`.
- B. Change the `login timeout`.
- C. Change the `idle-timeout`.
- D. Change the `udp idle timer`.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54 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 55

Refer to the exhibit.

```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
  pingsvr_flip_timeout/expire=3600s/2781s
    'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
    'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: `diagnose sys ha dump-by vcluster`.

Which two statements are true? (Choose two.)

- A. FortiGate SN FGVM010000065036 HA uptime has been reset.
- B. FortiGate devices are not in sync because one device is down.
- C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
- D. FortiGate SN FGVM010000064692 has the higher HA priority.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56 A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?

- A. The browser requires a software update.
- B. FortiGate does not support full SSL inspection when web filtering is enabled.
- C. The CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.
- D. There are network connectivity issues.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD41394>

QUESTION 57 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: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD34906>

QUESTION 58

Refer to the exhibit.



Network interface configuration

Edit Interface

Name

Alias

Type

Role

Address

Addressing mode Manual DHCP

IP/Netmask

Secondary IP address

Administrative Access

IPv4

HTTPS HTTP PING

FMG-Access SSH SNMP

TELNET FTM RADIUS Accounting

Security Fabric Connection

Receive LLDP Use VDOM Setting Enable Disable

Transmit LLDP Use VDOM Setting Enable Disable

Network

Device detection

Security mode Captive Portal

Authentication portal Local External

User Access Restricted to Groups Allow all

User Groups

Exempt sources

Exempt destinations/services

Redirect after Captive Portal Original Request Specific URL



```

Enforce authentication on demand option enabled
Local-FortiGate # config user setting
Local-FortiGate (setting) # show
config user setting
    set auth-cert "Fortinet_Factory"
    set auth-on-demand always
end
    
```

Firewall policies						
Name	Source	Destination	Schedule	Service	Action	NAT
LAN(port3) → WAN(port1) 2						
Sales Users	Sales LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled
Auth-Users	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled

The exhibit contains a network interface configuration, firewall policies, and a CLI console configuration.

How will FortiGate handle user authentication for traffic that arrives on the **LAN** interface?

- A. If there is a full-through policy in place, users will not be prompted for authentication.
- B. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.
- C. Authentication is enforced at a policy level; all users will be prompted for authentication.
- D. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59 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 60

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: ABD

Section: (none)

Explanation

Explanation/Reference:

