



**Fortinet**

## **Exam Questions NSE4\_FGT-7.2**

Fortinet NSE 4 - FortiOS 7.2

#### NEW QUESTION 1

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

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

**Answer:** BC

#### NEW QUESTION 2

Which statement is correct regarding the use of application control for inspecting web applications?

- A. Application control can identify child and parent applications, and perform different actions on them.
- B. Application control signatures are organized in a nonhierarchical structure.
- C. Application control does not require SSL inspection to identify web applications.
- D. Application control does not display a replacement message for a blocked web application.

**Answer:** A

#### NEW QUESTION 3

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

- A. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
- B. If a virus is detected, the last packet is delivered to the client.
- C. The IPS engine handles the process as a standalone.
- D. FortiGate buffers the whole file but transmits to the client at the same time.
- E. Flow-based inspection optimizes performance compared to proxy-based inspection.

**Answer:** ADE

#### NEW QUESTION 4

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 must the administrator make on FortiGate to meet the requirements? (Choose two.)

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

**Answer:** AD

#### NEW QUESTION 5

Which two statements are true about the FGCP protocol? (Choose two.)

- A. FGCP elects the primary FortiGate device.
- B. FGCP is not used when FortiGate is in transparent mode.
- C. FGCP runs only over the heartbeat links.
- D. FGCP is used to discover FortiGate devices in different HA groups.

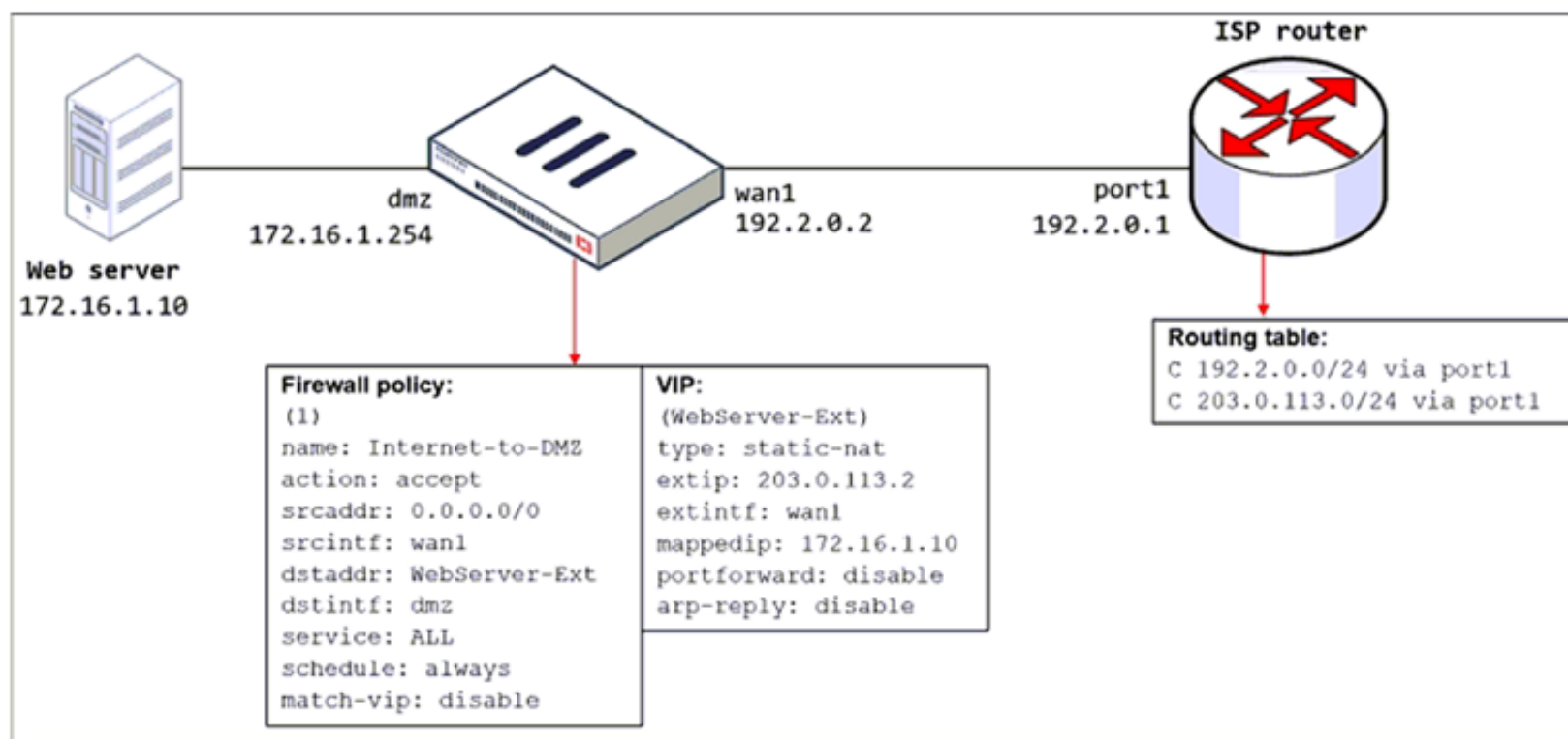
**Answer:** AD

#### NEW QUESTION 6

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?

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

**Answer: D**

#### NEW QUESTION 7

Refer to the exhibits.

The exhibits contain a network diagram, and virtual IP, IP pool, and firewall policies configuration information.

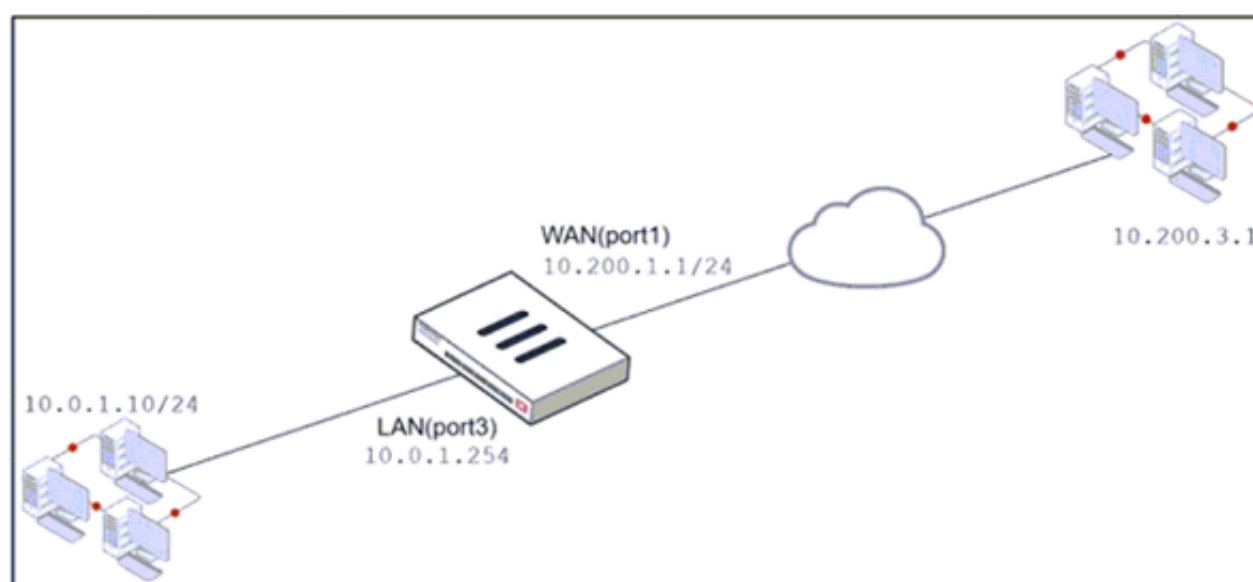
The WAN (port1) interface has the IP address 10.200.1.1/24.

The LAN (port3) interface has the IP address 10.0.1.254/24.

The first firewall policy has NAT enabled using IP pool.

The second firewall policy is configured with a VIP as the destination address.

#### Exhibit A Exhibit B



## Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	ACCEPT	IP Pool
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Disabled

### Edit Virtual IP

VIP type: IPv4

Name: VIP

Comments:  0/255

Color: [Change](#)

Network:

Interface: port1

Type: Static NAT

External IP address/range : 10.200.1.10

Map to:

IPv4 address/range: 10.0.1.10

☐ Optional Filters

☒ Port Forwarding

Protocol: **TCP** | UDP | SCTP | ICMP

Port Mapping Type: **One to one** | Many to many

External service port : 443

Map to IPv4 port: 443

### Edit Dynamic IP Pool

Name: IP Pool

Comments:  0/255

Type: **Overload** | One-to-One | Fixed Port Range | Port Block Allocation

External IP address/range : 10.200.1.100

NAT64: ☐

ARP Reply: ☒

Which IP address will be used to source NAT (SNAT) the internet traffic coming from a workstation with the IP address 10.0.1.10?

- A. 10.200.1.1  
B. 10.0.1.254  
C. 10.200.1.10  
D. 10.200.1.100

**Answer: D**

## NEW QUESTION 8

Refer to the exhibits.

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds.

## Exhibit B

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 3 hours, 28 minutes
```

## Exhibit B

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Based on the system performance output, which two results are correct? (Choose two.)

- A. FortiGate will start sending all files to FortiSandbox for inspection.
- B. FortiGate has entered conserve mode.
- C. Administrators cannot change the configuration.
- D. Administrators can access FortiGate only through the console port.

**Answer: BD**

## NEW QUESTION 9

Refer to the exhibits.

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook.

Users are given access to the Facebook web application. They can play video content hosted on

Facebook, but they are unable to leave reactions on videos or other types of posts.

Exhibit A Exhibit B

**Edit Policy**

Name	Facebook SSL Inspection
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Service	ALL

Firewall / Network Options

Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.

Security Profiles

SSL Inspection SSL certificate-inspection

Exhibit A Exhibit B

**Edit Policy**

Name	Facebook Access
Policy Mode	Standard Learn Mode
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	App Default Specify
Application	Facebook Facebook_Like.Button Facebook_Video.Play
URL Category	
Action	ACCEPT DENY

Firewall/Network Options

Protocol Options PROT default

Which part of the policy configuration must you change to resolve the issue?

- A. Force access to Facebook using the HTTP service.
- B. Make the SSL inspection a deep content inspection.
- C. Add Facebook in the URL category in the security policy.
- D. Get the additional application signatures required to add to the security policy.

Answer: B



#### NEW QUESTION 10

Refer to the exhibit.

```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 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=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
orgin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 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 contains a session diagnostic output. Which statement is true about the session diagnostic output?

- A. The session is in SYN\_SENT state.
- B. The session is in FIN\_ACK state.
- C. The session is in FTN\_WAIT state.
- D. The session is in ESTABLISHED state.

**Answer:** A

#### Explanation:

Indicates TCP (proto=6) session in SYN\_SENT state (proto=state=2) <https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

#### NEW QUESTION 10

Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

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

**Answer:** AC

#### NEW QUESTION 11

Which two statements are correct about NGFW Policy-based mode? (Choose two.)

- A. NGFW policy-based mode does not require the use of central source NAT policy
- B. NGFW policy-based mode can only be applied globally and not on individual VDOMs
- C. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy
- D. NGFW policy-based mode policies support only flow inspection

**Answer:** CD

#### NEW QUESTION 13

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.

Exhibit A Exhibit B

### Address Object

Name	Details
IP Range/Subnet 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN 5	
facebook.com	facebook.com

### Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services 1,633		
Facebook-Web	Destination	26,578
IP	Port	Protocol
1.9.91.17 - 1.9.91.18	80	TCP
	443	
	8443	
1.9.91.17 - 1.9.91.18	443	UDP
1.9.91.30	443	UDP

### Firewall Policies

ID	From	To	Source	Destination	Schedule	Service	Action	NAT
3	port3	port1	LOCAL_CLIENT	facebook.com	always	ULL_UDP	✓ ACCEPT	Enabled
1	port1	port3	facebook.com	LOCAL_CLIENT	always	ULL_UDP	✓ ACCEPT	Enabled
4	port4	port1	LOCAL_CLIENT	all	always	HTTP DNS HTTPS	✓ ACCEPT	Enabled
5	port3	port1	LOCAL_CLIENT	Facebook-Web	always	Internet Service	✓ ACCEPT	Enabled
2	port3	port1	all	all	always	ALL	✓ ACCEPT	Enabled

Exhibit A Exhibit B

### Policy Lookup

Incoming Interface

port3

IP Version

IPv4

Protocol

TCP

Source

10.0.1.10

Source Port

Optional (1-65535)

Destination

facebook.com

Destination Port

443

Search

Close

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

- A. Policy with ID 4.
- B. Policy with ID 5.
- C. Policies with ID 2 and 3.
- D. Policy with ID 4.

Answer: A

### NEW QUESTION 17

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

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

D. The NetSession Enum function is used to track user logouts.

**Answer:** D

**Explanation:**

FortiGate\_Infrastructure\_7.0 page 270: "NetAPI: polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function in Windows."

**NEW QUESTION 19**

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

**Answer:** ACD

**NEW QUESTION 20**

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

**Answer:** A

**NEW QUESTION 24**

Examine this PAC file configuration.

Which of the following statements are true? (Choose two.)

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.
- B. Any web request to the 172.25. 120.0/24 subnet is allowed to bypass the proxy.
- C. All requests not made to Fortinet.com or the 172.25. 120.0/24 subnet, have to go through altproxy.corp.com: 8060.
- D. Any web request fortinet.com is allowed to bypass the proxy.

**Answer:** AD

**NEW QUESTION 25**

Refer to the exhibit.

The exhibit shows the output of a diagnose command.



```
# diagnose firewall proute list
list route policy info(vf=root):
id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-02-23 05:46:43
```

What does the output reveal about the policy route?

- A. It is an ISDB route in policy route.
- B. It is a regular policy route.
- C. It is an ISDB policy route with an SDWAN rule.
- D. It is an SDWAN rule in policy route.

**Answer:** C

#### NEW QUESTION 29

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

**Answer:** ABE

#### Explanation:

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/739623/dns-filter-handled-by-ips-engine-in-flow>

#### NEW QUESTION 30

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.

**Answer:** ABD

#### Explanation:

When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:

- Incoming Interface
- Outgoing Interface
- Source: IP address, user, internet services
- Destination: IP address or internet services
- Service: IP protocol and port number
- Schedule: Applies during configured times

#### NEW QUESTION 34

A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) sub interfaces added to the physical interface. Which statements about the VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

- A. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.
- B. The two VLAN sub interfaces must have different VLAN IDs.
- C. The two VLAN sub interfaces can have the same VLAN ID, only if they belong to different VDOMs.
- D. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.

**Answer:** B

#### Explanation:

FortiGate\_Infrastructure\_6.0\_Study\_Guide\_v2-Online.pdf > page 147

"Multiple VLANs can coexist in the same physical interface, provide they have different VLAN ID"

#### NEW QUESTION 35

Which two statements explain antivirus scanning modes? (Choose two.)

- A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
- B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
- C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
- D. In flow-based inspection mode, files bigger than the buffer size are scanned.

**Answer:** BC

**Explanation:**

An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM--something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

**NEW QUESTION 40**

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

- A. hard-timeout
- B. auth-on-demand
- C. soft-timeout
- D. new-session
- E. Idle-timeout

**Answer:** ADE

**Explanation:**

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

**NEW QUESTION 41**

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.)

- A. www.example.com:443
- B. www.example.com
- C. example.com
- D. www.example.com/index.html

**Answer:** BC

**Explanation:**

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 43**

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.

**Answer:** C

**Explanation:**

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

#### NEW QUESTION 47

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

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

☐

Edit AntiVirus Profile

Name

default

Comments

Scan files and block viruses.
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

*i*

Use FortiGuard Outbreak Prevention Database

☐

Use External Malware Block List

*i*
☐

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 firewall policy performs the full content inspection on the file.
- B. The flow-based inspection is used, which resets the last packet to the user.
- C. The volume of traffic being inspected is too high for this model of FortiGate.



D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer: B

Explanation:

· "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately

· When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.

In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

NEW QUESTION 51

Refer to the exhibits.

The exhibits show a network diagram and firewall configurations.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver. Remote-User2 must not be able to access the Webserver.

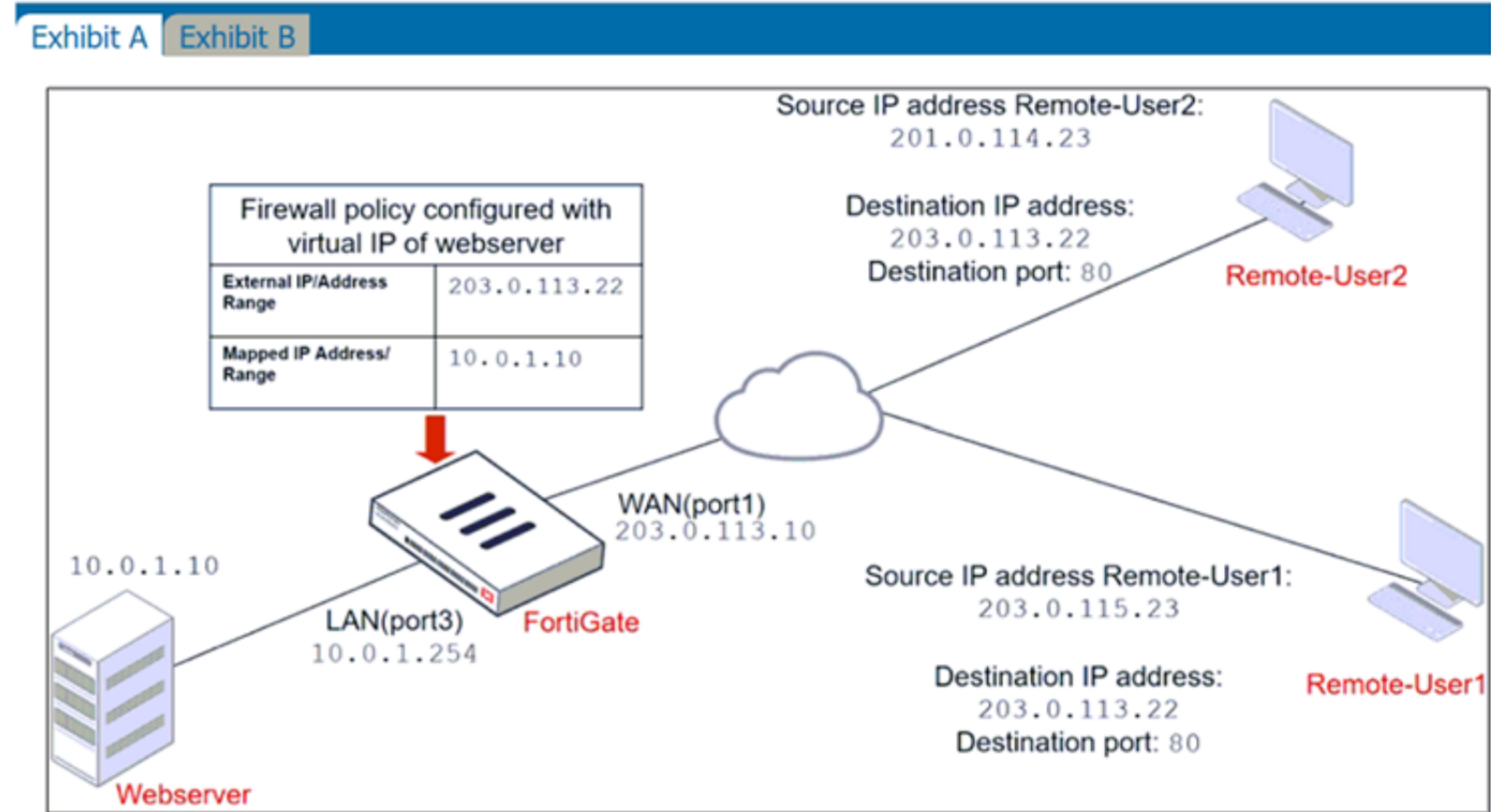


Exhibit A   Exhibit B

Edit Address

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 web server access. 23/255

Firewall address object

Firewall policies

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

In this scenario, 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.

Answer: CD

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta>



### NEW QUESTION 55

Refer to the exhibits.

Exhibit A shows a topology for a FortiGate HA cluster that performs proxy-based inspection on traffic. Exhibit B shows the HA configuration and the partial output of the get system ha status command.

Exhibit A Exhibit B

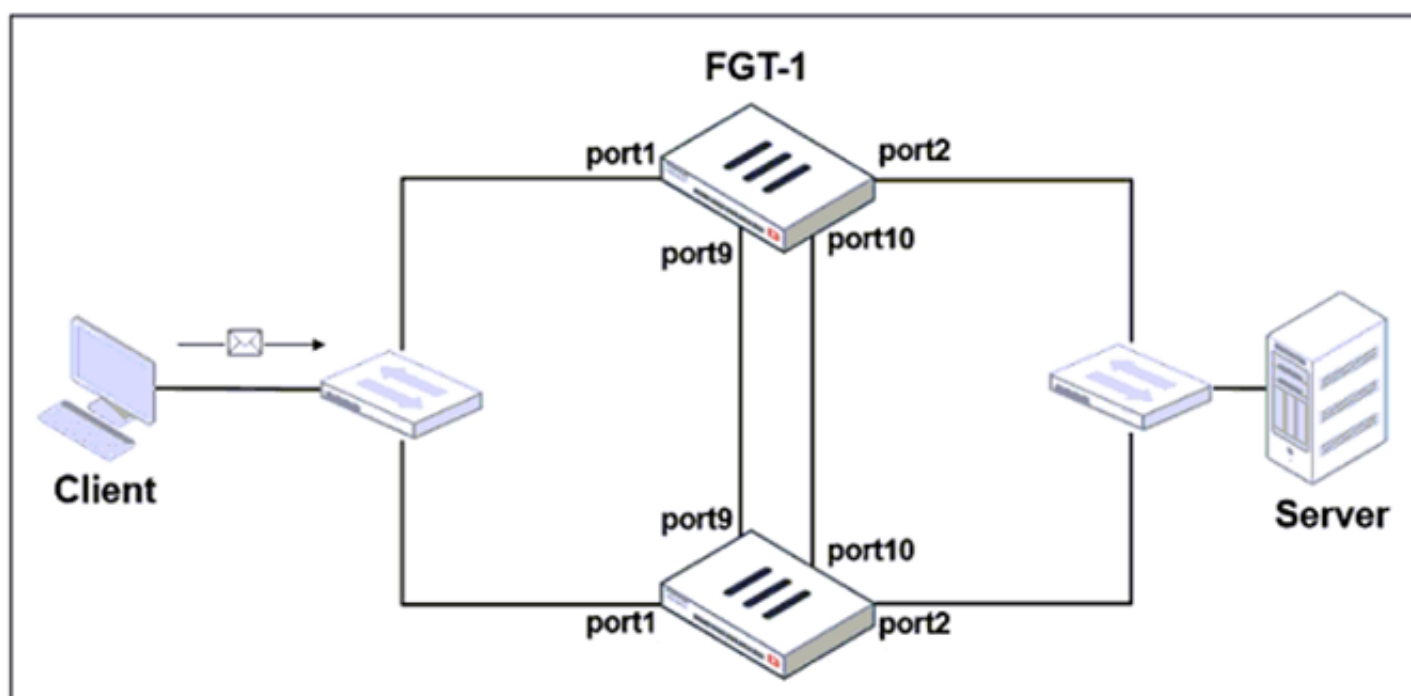


Exhibit A Exhibit B

```
set group-id 3
set group-name "NSE"
set mode a-a
set password *
set hbdev "port9" 50 "port10" 50
set session-pickup enable
set override disable
set monitor port3
end

# get system ha status
...
Primary      : FGT-2, FGVM010000065036, HA cluster index = 1
Secondary    : FGT-1, FGVM010000064692, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000065036, HA operating index = 1
Secondary: FGVM010000064692, HA operating index = 0
```

Based on the exhibits, which two statements about the traffic passing through the cluster are true? (Choose two.)

- A. For non-load balanced connections, packets forwarded by the cluster to the server contain the virtual MAC address of port2 as source.
- B. The traffic sourced from the client and destined to the server is sent to FGT-1.
- C. The cluster can load balance ICMP connections to the secondary.
- D. For load balanced connections, the primary encapsulates TCP SYN packets before forwarding them to the secondary.

Answer: AB

### NEW QUESTION 56

An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

- A. The strict RPF check is run on the first sent and reply packet of any new session.
- B. Strict RPF checks the best route back to the source using the incoming interface.
- C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
- D. Strict RPF allows packets back to sources with all active routes.

Answer: C

### NEW QUESTION 60

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 192.168. 1.0/24 and the remote quick mode selector is 192.168.2.0/24. Which subnet must the administrator configure for the local quick mode selector for site B?

- A. 192.168.3.0/24
- B. 192.168.2.0/24
- C. 192.168. 1.0/24
- D. 192.168.0.0/8

Answer: C

#### NEW QUESTION 61

An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings. What is true about the DNS connection to a FortiGuard server?

- A. It uses UDP 8888.
- B. It uses UDP 53.
- C. It uses DNS over HTTPS.
- D. It uses DNS over TLS.

Answer: B

#### NEW QUESTION 65

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%.

Answer: C

#### NEW QUESTION 68

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporally disabled while upgrading the firmware.

Answer: CD

#### NEW QUESTION 69

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

- A. Configure Source IP Pools.
- B. Configure split tunneling in tunnel mode.
- C. Configure different SSL VPN realms.
- D. Configure host check .

Answer: D

#### NEW QUESTION 71

Refer to the exhibits.  
 Exhibit A.

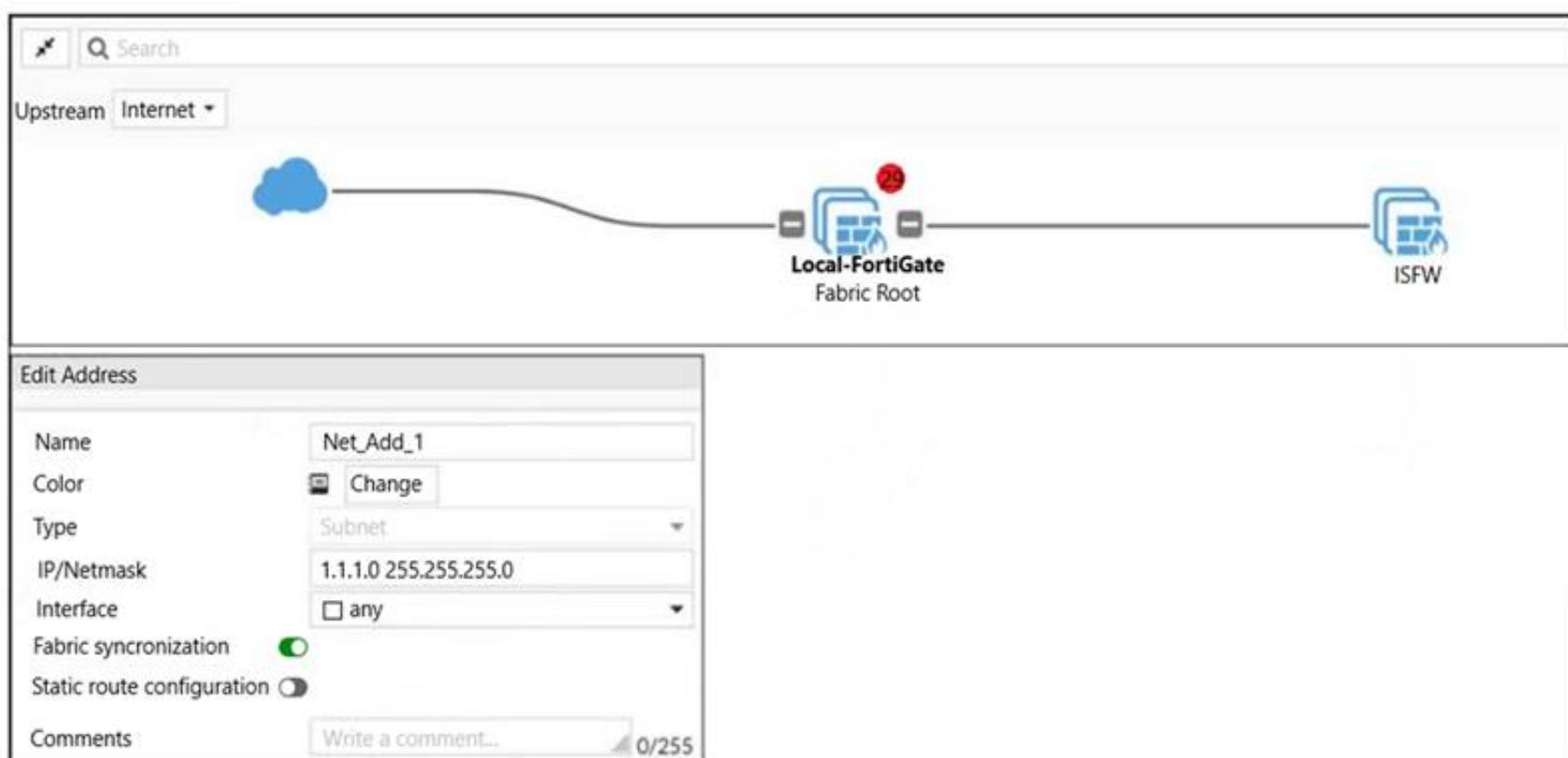


Exhibit B.

```
Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 0.0.0.0
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC X18CtzrcUBUq9yz9nryP+YfM16
    BJkv7S/trtoh2gYAe5CH8YMAa0GT18aX+/dKH/o5izw1ZEoN1QN2N
    FGLT4r5z2AyYI8i1PxutiLcsCp1AdZadv1CxDe66IdLX7I6o22J9P
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set fabric-object-unification local
    set saml-configuration-sync default
```

```
ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 10.0.1.254
    set upstream-port 8013
    set group-name ''
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync default
end

ISFW #
ISFW #
```

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?

- A. Change the csf setting on Local-FortiGate (root) to set configuration-sync local.
- B. Change the csf setting on ISFW (downstream) to set configuration-sync local.
- C. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.
- D. Change the csf setting on ISFW (downstream) to set fabric-object-unification default.

**Answer:** C

#### NEW QUESTION 74

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

- A. Warning
- B. Exempt
- C. Allow
- D. Learn

**Answer:** AC

#### NEW QUESTION 75

Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- A. diagnose wad session list
- B. diagnose wad session list | grep hook-pre&&hook-out
- C. diagnose wad session list | grep hook=pre&&hook=out
- D. diagnose wad session list | grep "hook=pre"&"hook=out"

**Answer:** A

#### NEW QUESTION 79

Which of the following SD-WAN load balancing method use interface weight value to distribute traffic? (Choose two.)

- A. Source IP
- B. Spillover
- C. Volume
- D. Session

**Answer:** CD

#### Explanation:

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/49719/configuring-sd-wan-load-balancing>

#### NEW QUESTION 80

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NSE4\_FGT-7.2 Practice Exam Features:

- \* NSE4\_FGT-7.2 Questions and Answers Updated Frequently
- \* NSE4\_FGT-7.2 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE4\_FGT-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE4\_FGT-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE4\\_FGT-7.2 Practice Test Here](#)**