

Fortinet

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2



NEW QUESTION 1

Refer to exhibit.

An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.

FortiGuard Category Based Filter

Name	Action
Medicine	Allow
News and Media	Allow
Social Networking	Block
Political Organizations	Allow
Reference	Allow
Global Religion	Allow
Shopping	Allow
Society and Lifestyles	Allow
Sports	Allow

Static URL Filter

Block invalid URLs: ☐

URL Filter: ☒

URL	Type	Action	Status
twitter.com	Wildcard	Allow	Enable

Block malicious URLs discovered by FortiSandbox: ☐

Content Filter: ☐

Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

- A. On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking
- B. On the Static URL Filter configuration, set Type to Simple
- C. On the Static URL Filter configuration, set Action to Exempt.
- D. On the Static URL Filter configuration, set Action to Monitor.

Answer: C

NEW QUESTION 2

Which statement about the IP authentication header (AH) used by IPsec is true?

- A. AH does not provide any data integrity or encryption.
- B. AH does not support perfect forward secrecy.
- C. AH provides data integrity but no encryption.
- D. AH provides strong data integrity but weak encryption.

Answer: C

NEW QUESTION 3

When configuring a firewall virtual wire pair policy, which following statement is true?

- A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
- B. Only a single virtual wire pair can be included in each policy.
- C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
- D. Exactly two virtual wire pairs need to be included in each policy.

Answer: A

NEW QUESTION 4

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scope of application control to the browser-based technology category only.
- B. It limits the scope of application control to scan application traffic based on application category only.
- C. It limits the scope of application control to scan application traffic using parent signatures only
- D. It limits the scope of application control to scan application traffic on DNS protocol only.

Answer: B

NEW QUESTION 5

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 6

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 7

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 8

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 9

Refer to the exhibit.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack .
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

Answer: A

NEW QUESTION 10

Refer to the exhibit.



The screenshot shows the FortiGate SLA configuration interface. The 'Name' field is set to 'SLA1'. Under 'Protocol', 'Ping' is selected. The 'Server' field contains two entries: '4.2.2.2' and '4.2.2.1'. Under 'Participants', 'All SD-WAN Members' is selected. There are two checkboxes for 'port1' and 'port2', both of which are unchecked. At the bottom, there is a toggle switch 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 sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

- A. The Detection Mode setting is not set to Passive.
- B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
- C. The configured participants are not SD-WAN members.
- D. The Enable probe packets setting is not enabled.

Answer: BD

NEW QUESTION 10

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**

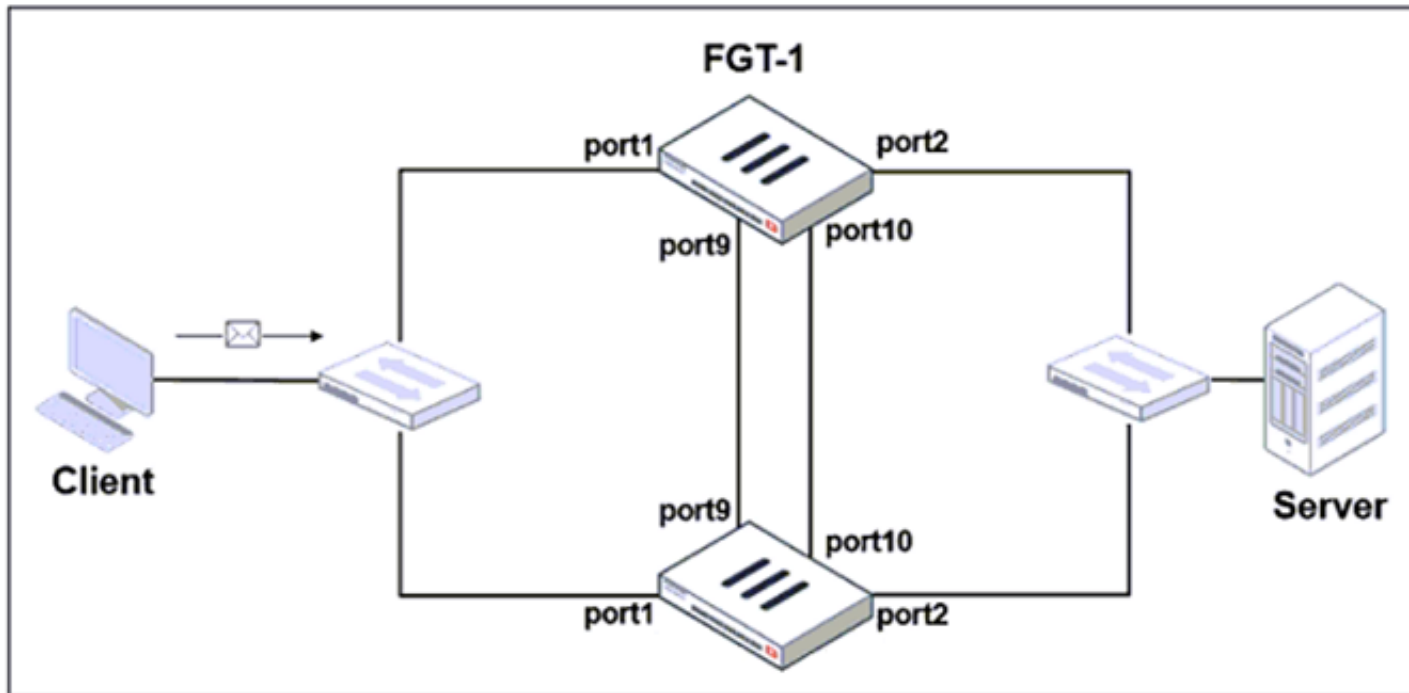


Exhibit A **Exhibit B**

```
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 13

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

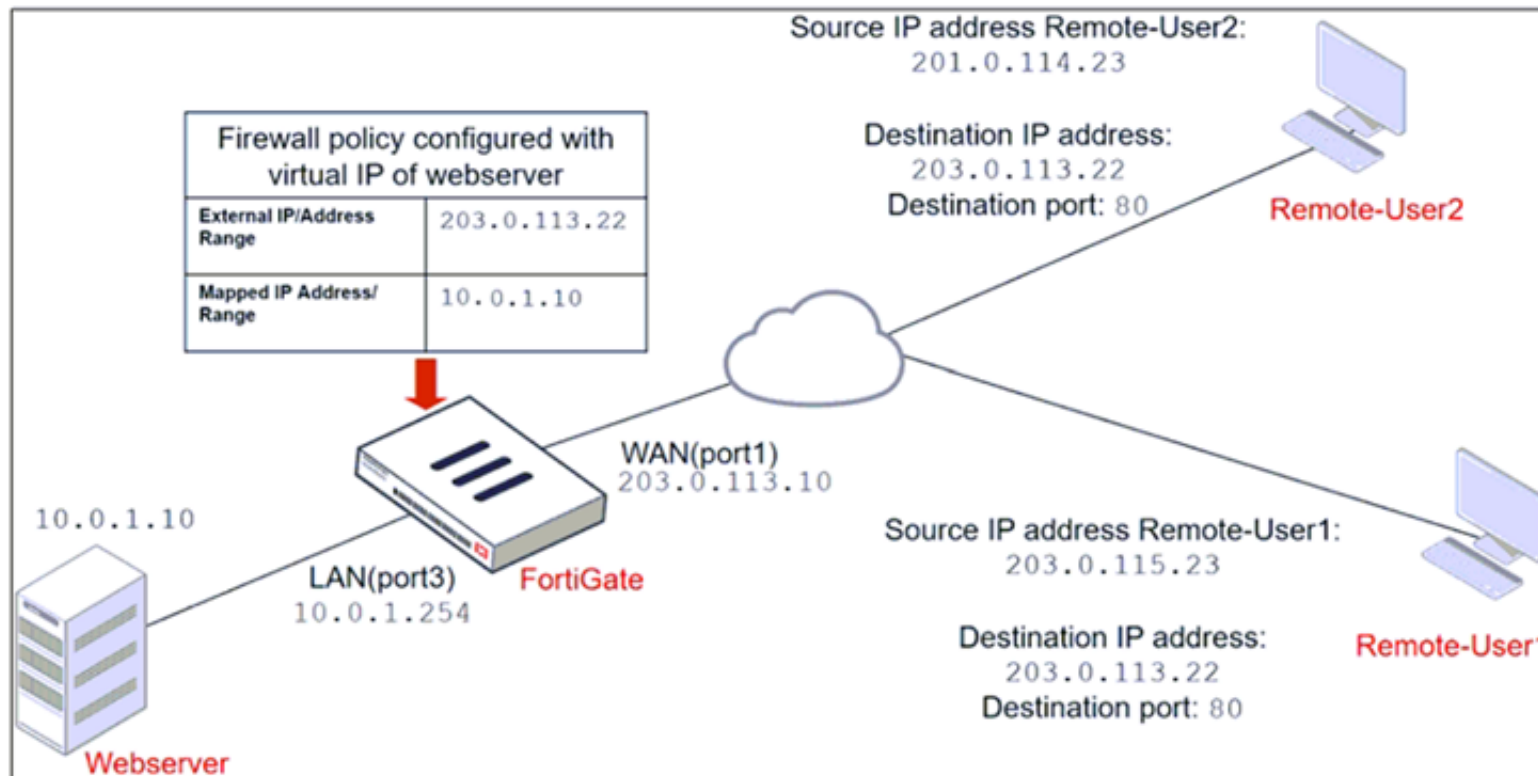


Exhibit A Exhibit B

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 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.

Answer: C

Explanation:

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

NEW QUESTION 17

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 20

Which two statements are correct about a software switch on FortiGate? (Choose two.)

- A. It can be configured only when FortiGate is operating in NAT mode
- B. Can act as a Layer 2 switch as well as a Layer 3 router
- C. All interfaces in the software switch share the same IP address
- D. It can group only physical interfaces

Answer: AC

NEW QUESTION 23

Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

- A. Heartbeat interfaces have virtual IP addresses that are manually assigned.
- B. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.
- C. Virtual IP addresses are used to distinguish between cluster members.
- D. The primary device in the cluster is always assigned IP address 169.254.0.1.

Answer: BD

NEW QUESTION 27

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 31

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 34

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scanning of application traffic to the DNS protocol only.
- B. It limits the scanning of application traffic to use parent signatures only.
- C. It limits the scanning of application traffic to the browser-based technology category only.
- D. It limits the scanning of application traffic to the application category only.

Answer: C

Explanation:

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

NEW QUESTION 38

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 40

In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

- A. The IP version of the sources and destinations in a firewall policy must be different.
- B. The Incoming Interfac
- C. Outgoing Interfac
- D. Schedule, and Service fields can be shared with both IPv4 and IPv6.
- E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
- F. The IP version of the sources and destinations in a policy must match.
- G. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: BDE

NEW QUESTION 45

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 49

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 51

Refer to the exhibit.

```
FGT1 # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

S      *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
        *>          [10/0] via 10.0.0.2, port2, [30/0]
S      0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C      *> 10.0.0.0/24 is directly connected, port2
S      172.13.24.0/24 [10.0] is directly connected, port4
C      *> 172.20.121.0/24 is directly connected, port1
S      *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C      *> 192.168.15.0/24 is directly connected, port3
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

- A. The port3 default route has the highest distance.
- B. The port3 default route has the lowest metric.
- C. There will be eight routes active in the routing table.
- D. The port1 and port2 default routes are active in the routing table.

Answer: AD

NEW QUESTION 53

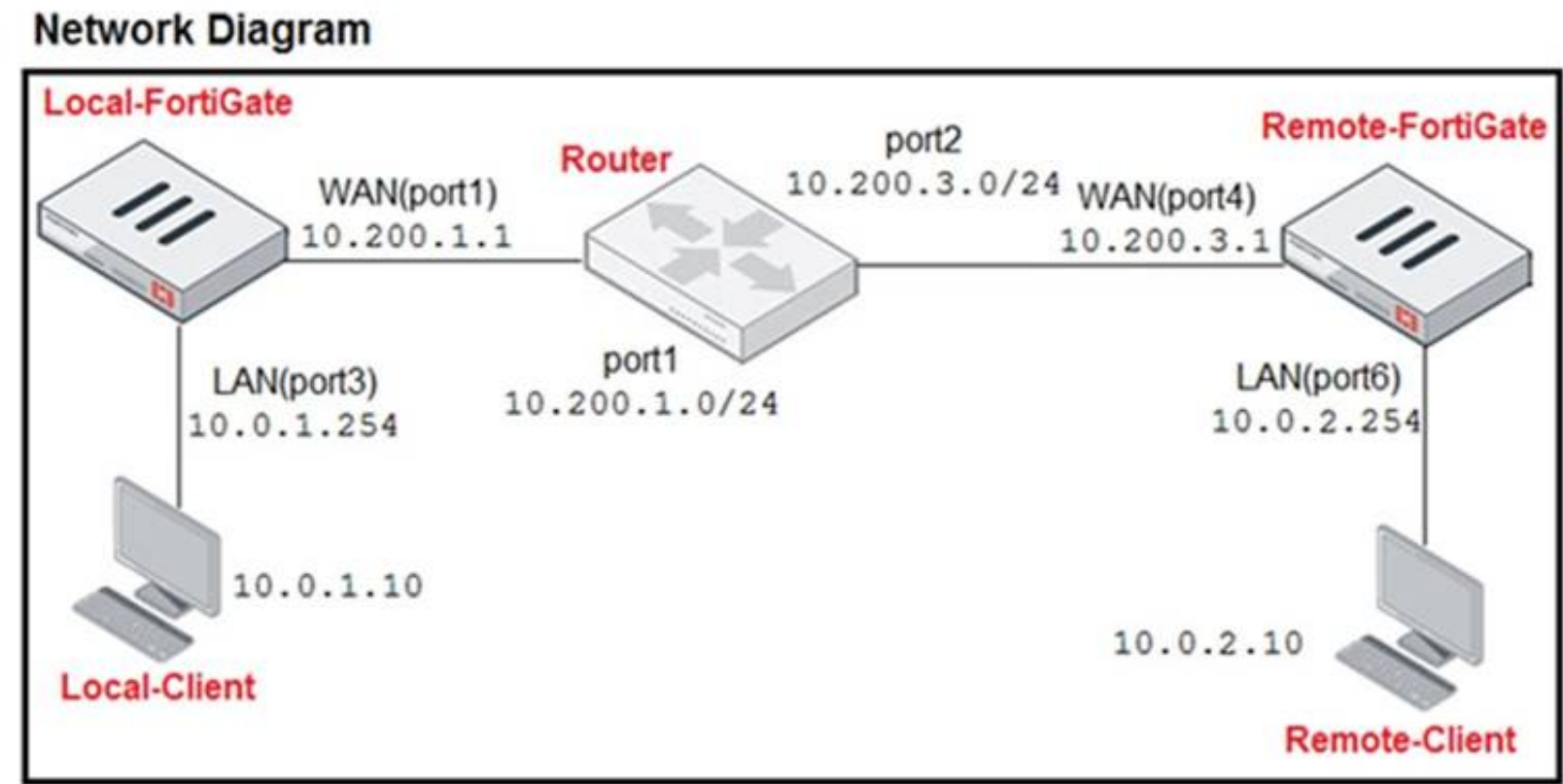
Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

- A. By default, FortiGate uses WINS servers to resolve names.
- B. By default, the SSL VPN portal requires the installation of a client's certificate.
- C. By default, split tunneling is enabled.

D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer: D

NEW QUESTION 54
Refer to the exhibit.



Central SNAT Policies Local-FortiGate

<div> <div>+ Create New</div> <div>Edit</div> <div>Delete</div> <div>Search</div> <div>Q</div> </div>						
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

<div> <div>+ Create New</div> <div>Edit</div> <div>Clone</div> <div>Delete</div> <div>Search</div> <div>Q</div> </div>			
Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	Enabled

Protocol Number Table

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

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration. The WAN (port1) interface has the IP address 10.200. 1. 1/24. The LAN (port3) interface has the IP address 10.0. 1.254/24. A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied. Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0. 1. 10) pings the IP address of Remote-FortiGate (10.200.3. 1)?

- A. 10.200. 1. 149
- B. 10.200. 1. 1
- C. 10.200. 1.49
- D. 10.200. 1.99

Answer: D

NEW QUESTION 55

An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

- A. Device detection on all interfaces is enforced for 30 minutes.
- B. Denied users are blocked for 30 minutes.
- C. The number of logs generated by denied traffic is reduced.
- D. A session for denied traffic is created.

Answer: AC

NEW QUESTION 60

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 63

Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

What two conclusions can you make from the debug flow output? (Choose two.)

- A. The debug flow is for ICMP traffic.
- B. The default route is required to receive a reply.
- C. A new traffic session was created.
- D. A firewall policy allowed the connection.

Answer: AC

NEW QUESTION 68

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**

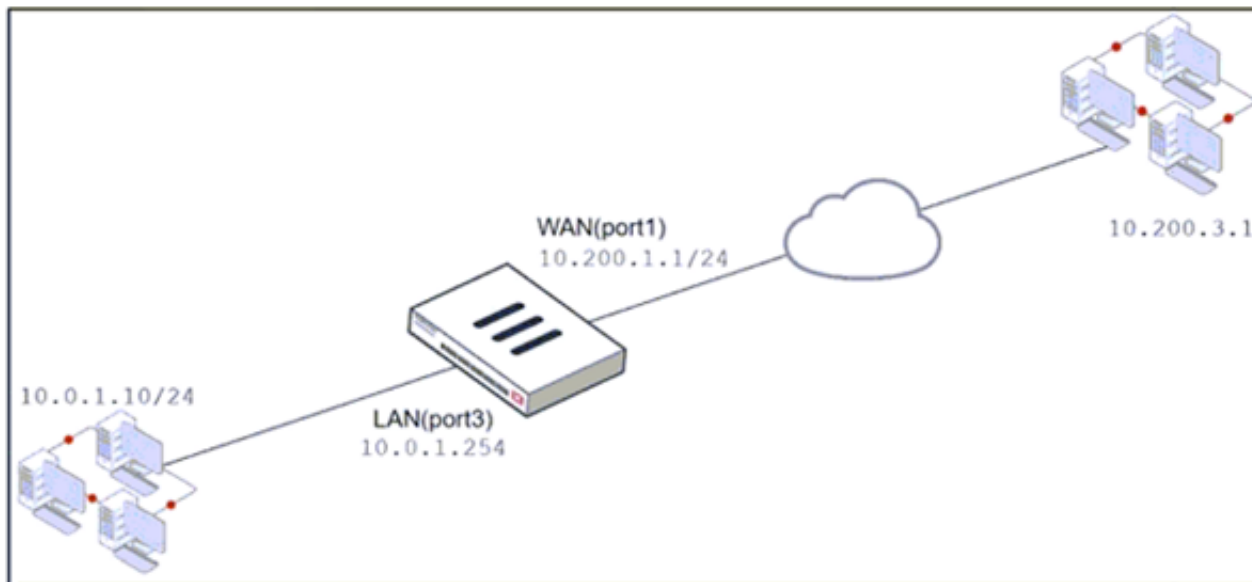


Exhibit A **Exhibit B**

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: Write a comment... 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: Write a comment... Type: Overload One-to-One Fixed Port Range Port Block Allocation External IP address/range: 10.200.1.100-10.200.1.100 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 73

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 77

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 78

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 82

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 84

A network administrator enabled antivirus and selected an SSL inspection profile on a firewall policy. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and does not block the file, allowing it to be downloaded.

The administrator confirms that the traffic matches the configured firewall policy.

What are two reasons for the failed virus detection by FortiGate? (Choose two.)

- A. The website is exempted from SSL inspection.
- B. The EICAR test file exceeds the protocol options oversize limit.
- C. The selected SSL inspection profile has certificate inspection enabled.
- D. The browser does not trust the FortiGate self-signed CA certificate.

Answer: AD

NEW QUESTION 87

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

Answer: BDE

NEW QUESTION 91

.....

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](#)