



Fortinet

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

NEW QUESTION 1

Refer to the exhibits.
Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object 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.

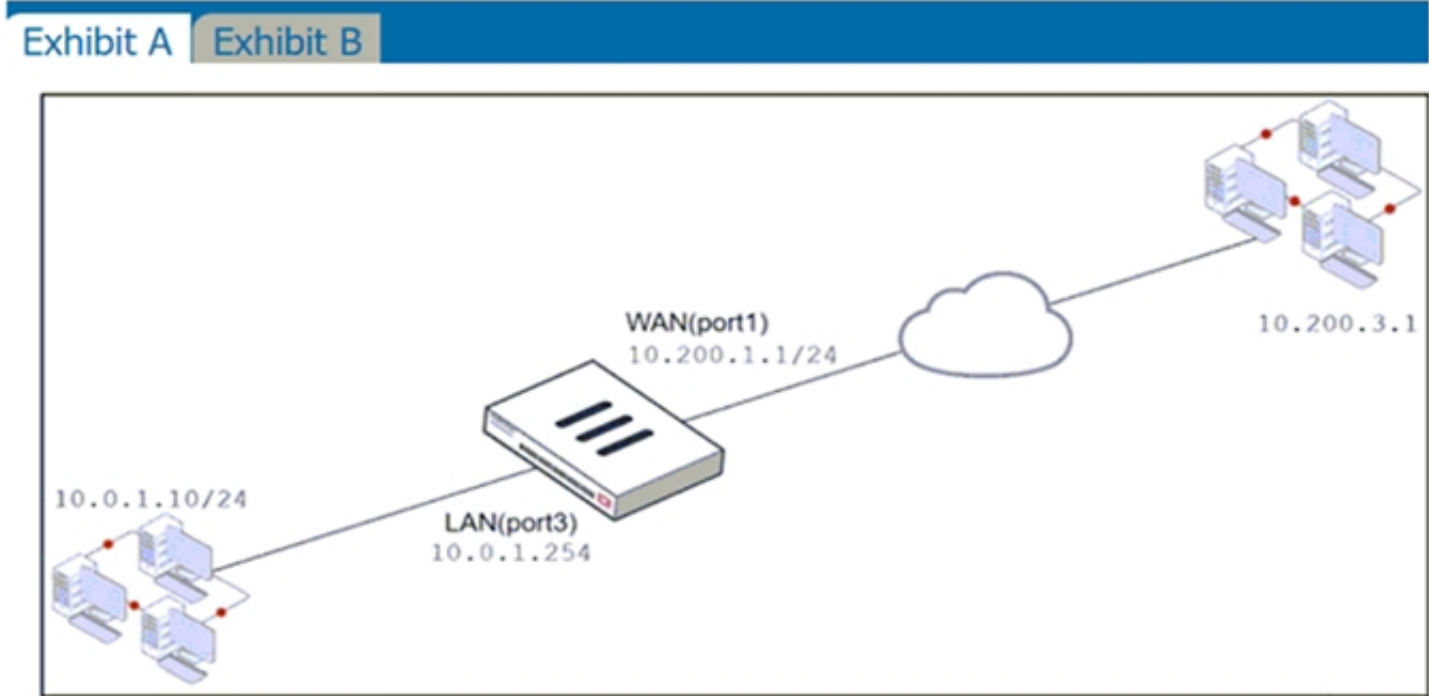


Exhibit A Exhibit B

| Name | From | To | Source | Destination | Schedule | Service | Action | NAT |
|-----------|-------------|-------------|--------|-------------|----------|---------|--------|---------|
| WebServer | WAN (port1) | LAN (port3) | all | VIP | always | ALL | ACCEPT | Enabled |

Edit Virtual IP

VIP type: IPv4

Name: VIP

Comments: Write a comment... 0/255

Color: Change

Network

Interface: WAN (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: 10443

Map to IPv4 port: 443

- If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?
- A. 10.0.1.254, 10.0.1.10, and 443, respectively
 - B. 10.0.1.254, 10.0.1.10, and 10443, respectively
 - C. 10.200.3.1, 10.0.1.10, and 443, respectively

Answer: C

NEW QUESTION 2

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 3

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 4

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 5

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 6

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 7

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 8

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 9

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]
S      *>          [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 10

Refer to the web filter raw logs.


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

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

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

- A. 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 10

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 Interface
- C. Outgoing Interface
- 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 15

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 19

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 23

Refer to the exhibit.



The screenshot shows the FortiGate SLA configuration interface. The 'Name' field is set to 'SLA1'. The 'Protocol' is set to 'Ping'. The 'Server' field has two entries: '4.2.2.2' and '4.2.2.1'. The 'Participants' field is set to 'All SD-WAN Members'. The 'Enable probe packets' checkbox is unchecked. There are also buttons for 'Specify' and a list of participants including 'port1' and 'port2'.

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 28

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 29

Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- A. FortiCache
- B. FortiSIEM
- C. FortiAnalyzer
- D. FortiSandbox
- E. FortiCloud

Answer: BCE

NEW QUESTION 30

Refer to the exhibits.
Exhibit A.

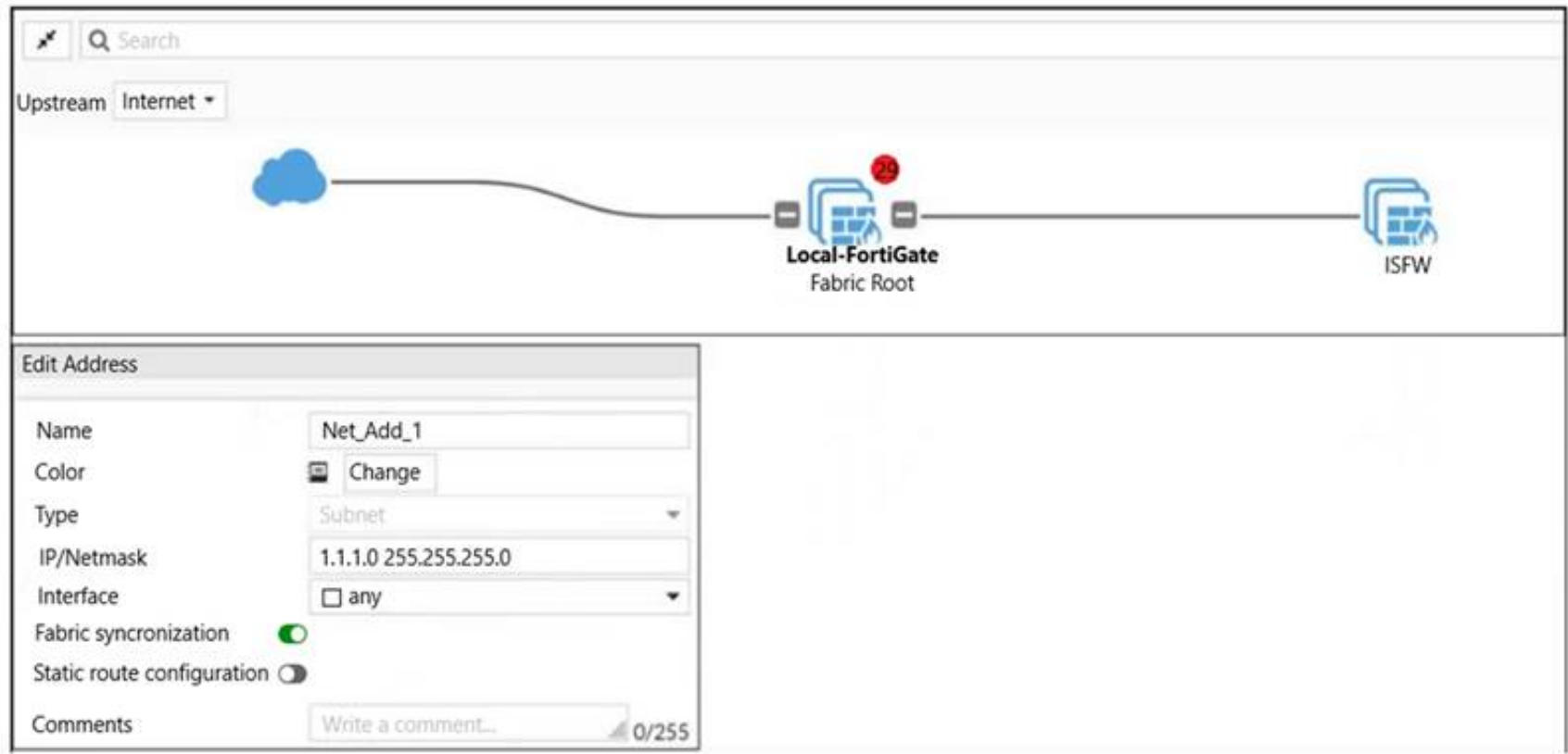


Exhibit B.

```

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 31

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 35

.....

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](#)