

## Exam Questions NSE4\_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

[https://www.2passeasy.com/dumps/NSE4\\_FGT-7.2/](https://www.2passeasy.com/dumps/NSE4_FGT-7.2/)



#### NEW QUESTION 1

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 2

Which two attributes are required on a certificate so it can be used as a CA certificate on SSL inspection? (Choose two.)

- A. The keyUsage extension must be set to keyCertSign.
- B. The CA extension must be set to TRUE.
- C. The issuer must be a public CA.
- D. The common name on the subject field must use a wildcard name.

**Answer:** AB

#### NEW QUESTION 3

Which timeout setting can be responsible for deleting SSL VPN associated sessions?

- A. SSL VPN idle-timeout
- B. SSL VPN http-request-body-timeout
- C. SSL VPN login-timeout
- D. SSL VPN dtls-hello-timeout

**Answer:** A

#### 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 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

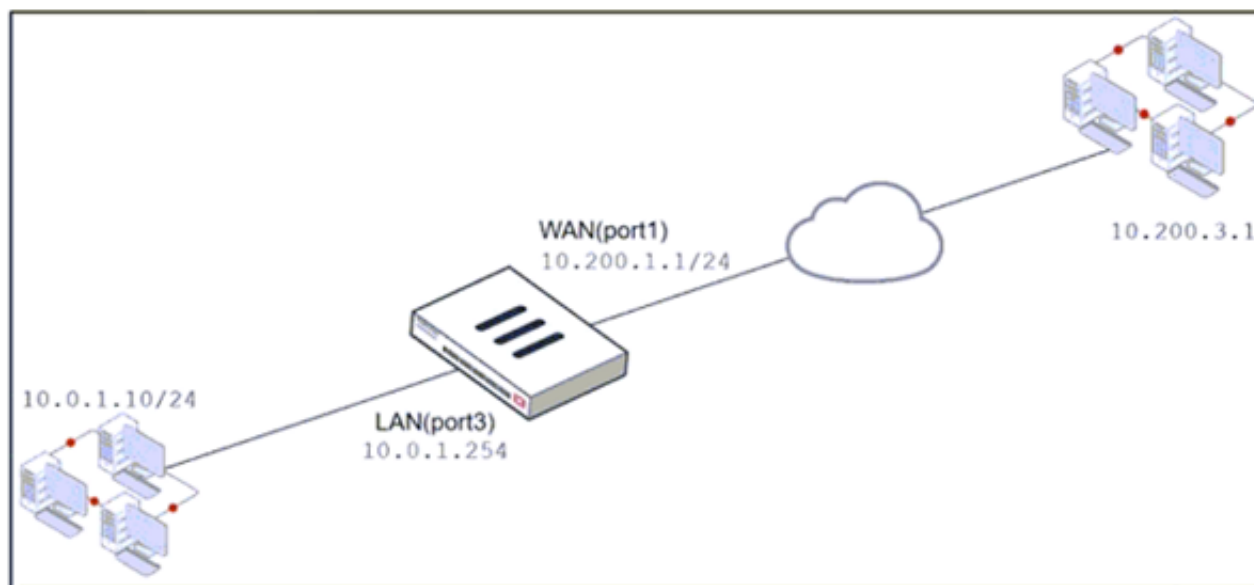


Exhibit A Exhibit B

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		Edit Dynamic IP Pool	
VIP type	IPv4	Name	IP Pool
Name	VIP	Comments	Write a comment...
Comments	Write a comment...	Type	Overload One-to-One Fixed Port Range Port Block Allocation
Color	Change	External IP address/range	10.200.1.100-10.200.1.100
Network		NAT64	
Interface	port1	ARP Reply	
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		

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 7

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 8

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 9

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 10

Refer to the exhibit.

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

Answer: D

#### Explanation:

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

#### NEW QUESTION 10

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 15



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 19**

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
rpd_b_link_id= 00000000 rpd_b_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:**

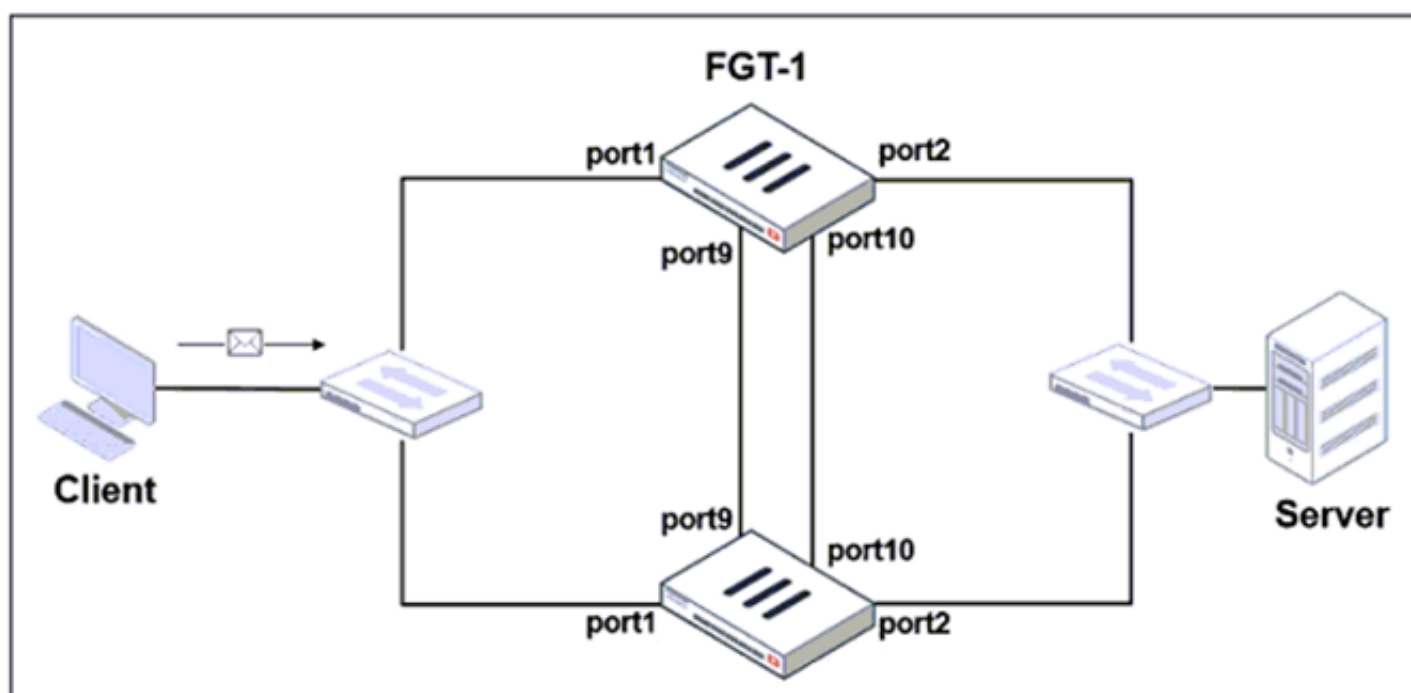
<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

**NEW QUESTION 21**

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 22

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 24

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 29

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 33

An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

- A. Policy lookup will be disabled.
- B. By Sequence view will be disabled.
- C. Search option will be disabled
- D. Interface Pair view will be disabled.

**Answer:** D

### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821>

### NEW QUESTION 38

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 39**

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 40**

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 bur no encryption.
- D. AH provides strong data integrity but weak encryption.

**Answer:** C

**NEW QUESTION 42**

If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

- A. A CRL
- B. A person
- C. A subordinate CA
- D. A root CA

**Answer:** D

**NEW QUESTION 44**

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4\_FGT-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4\_FGT-7.2 Product From:

[https://www.2passeasy.com/dumps/NSE4\\_FGT-7.2/](https://www.2passeasy.com/dumps/NSE4_FGT-7.2/)

## Money Back Guarantee

### 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