

## Exam Questions NSE4\_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

[https://www.2passeasy.com/dumps/NSE4\\_FGT-7.0/](https://www.2passeasy.com/dumps/NSE4_FGT-7.0/)



### NEW QUESTION 1

If Internet Service is already selected as Destination in a firewall policy, which other configuration object can be selected for the Destination field of a firewall policy?

- A. IP address
- B. No other object can be added
- C. FQDN address
- D. User or User Group

**Answer: B**

#### Explanation:

FortiGate Security 7.2 Study Guide (p.59): "When configuring your firewall policy, you can use Internet Service as the destination in a firewall policy, which contains all the IP addresses, ports, and protocols used by that service. For the same reason, you cannot mix regular address objects with ISDB objects, and you cannot select services on a firewall policy. The ISDB objects already have services information, which is hardcoded."

This is true because Internet Service is a special type of destination object that can only be used alone in a firewall policy. Internet Service is a feature that allows FortiGate to identify and filter traffic based on the internet service or application that it belongs to, such as Facebook, YouTube, Skype, etc. Internet Service uses a database of IP addresses and ports that are associated with each internet service or application, and updates it regularly from FortiGuard. When Internet Service is selected as the destination in a firewall policy, FortiGate will match the traffic to the corresponding internet service or application, and apply the appropriate action and security profiles to it. However, Internet Service cannot be combined with any other destination object, such as IP address, FQDN address, user or user group, etc., as this would create a conflict or ambiguity in the firewall policy. Therefore, no other object can be added if Internet Service is already selected as the destination in a firewall policy

### NEW QUESTION 2

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

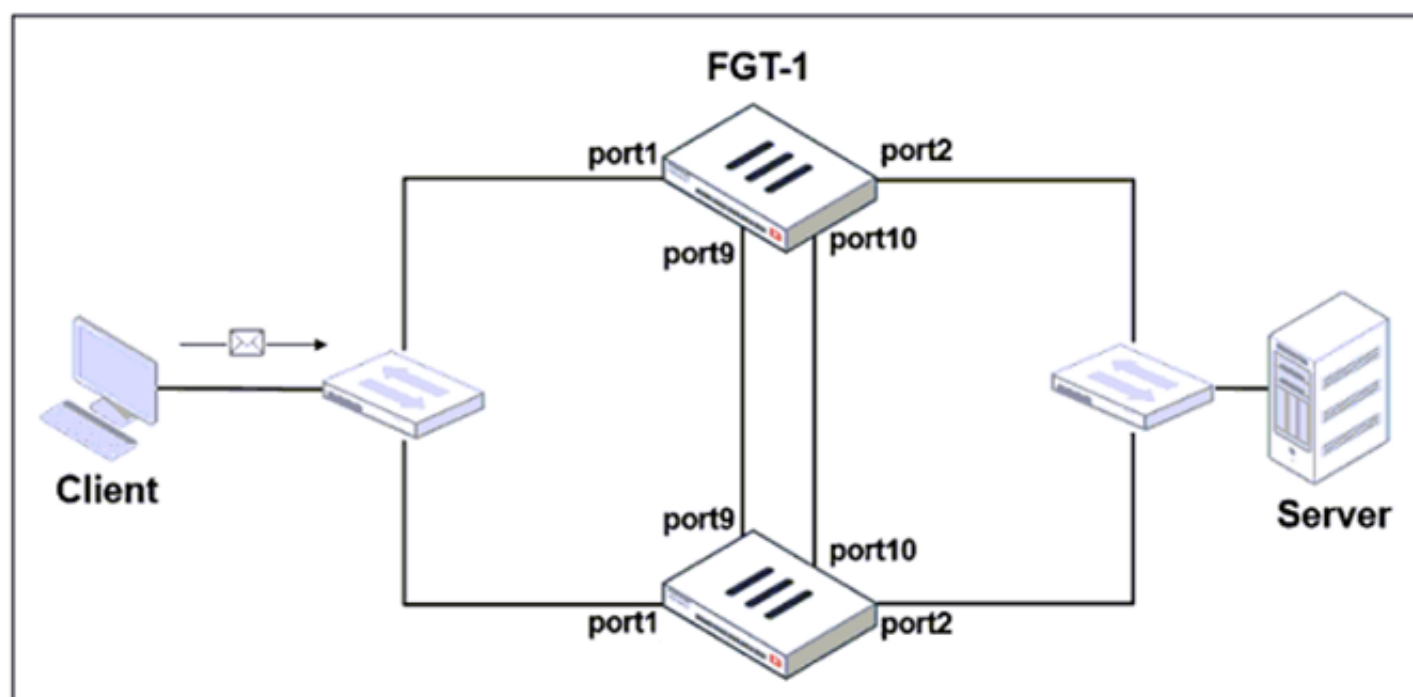


Exhibit A Exhibit B

```

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: AD

#### Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.317 & p.320): "To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses." "The primary forwards the SYN packet to the selected secondary. (...) This is also known as MAC address rewrite. In addition, the primary encapsulates the packet in an Ethernet frame type 0x8891. The encapsulation is done only for the first packet of a load balanced session. The encapsulated packet includes the original packet plus session information that the secondary requires to process the traffic."

#### NEW QUESTION 3

Refer to the exhibit.

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.



Based on the phase 2 configuration shown in the exhibit, which configuration change will bring phase 2 up?

- A. On Remote-FortiGate, set Seconds to 43200.
- B. On HQ-FortiGate, set Encryption to AES256.
- C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
- D. On HQ-FortiGate, enable Auto-negotiate.

Answer: B

#### NEW QUESTION 4

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-Filter
Status      : Enable
License     : Contract

Num. of servers : 3
Protocol     : https
Port        : 443
Anycast     : Disable
Default servers : Included
-- Server List (Mon Jul 5 12:00:25 2021) --

IP           Weight  RTT  Flags  TZ  FortiGuard-requests  Curr Lost Total Lost  Updated Time
173.243.138.210  10    350  DI    -8    29      0      0      0      Mon Jul 5 09:23:33 2021
12.34.97.18     20     30   -5    -5    25      0      0      0      Mon Jul 5 09:23:33 2021
210.7.96.18     160   605   9     9    25      0      0      0      Mon Jul 5 09:23:33 2021
```

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

- A. A local FortiManager is one of the servers FortiGate communicates with.
- B. One server was contacted to retrieve the contract information.
- C. There is at least one server that lost packets consecutively.
- D. FortiGate is using default FortiGuard communication settings.

Answer: BD

#### Explanation:

FortiGate Security 7.2 Study Guide (p.287-288): "Flags: D (IP returned from DNS), I (Contract server contacted), T (being timed), F (failed)" "By default, FortiGate is configured to enforce the use of HTTPS port 443 to perform live filtering with FortiGuard or FortiManager. Other ports and protocols are available by disabling the FortiGuard anycast setting on the CLI."

#### NEW QUESTION 5

An administrator is configuring an IPsec VPN between site A and site B. The Remote 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. 1.0/24
- B. 192. 168.0.0/24
- C. 192. 168.2.0/24
- D. 192. 168.3.0/24

**Answer:** C

#### Explanation:

For an IPsec VPN between site A and site B, the administrator has configured the local quick mode selector for site A as 192.168.1.0/24 and the remote quick mode selector as 192.168.2.0/24. This means that the VPN will allow traffic to and from the 192.168.1.0/24 subnet at site A to reach the 192.168.2.0/24 subnet at site B.

To complete the configuration, the administrator must configure the local quick mode selector for site B. To do this, the administrator must use the same subnet as the remote quick mode selector for site A, which is 192.168.2.0/24. This will allow traffic to and from the 192.168.2.0/24 subnet at site B to reach the 192.168.1.0/24 subnet at site A.

Therefore, the administrator must configure the local quick mode selector for site B as 192.168.2.0/24.

#### NEW QUESTION 6

Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

- A. Antivirus engine
- B. Intrusion prevention system engine
- C. Flow engine
- D. Detection engine

**Answer:** B

#### Explanation:

<http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control>

#### NEW QUESTION 7

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 8

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 9

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

- A. IP address
- B. Once Internet Service is selected, no other object can be added
- C. User or User Group
- D. FQDN address

**Answer:** B

#### NEW QUESTION 10

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 10

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 12

Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up. but phase 2 fails to come up.

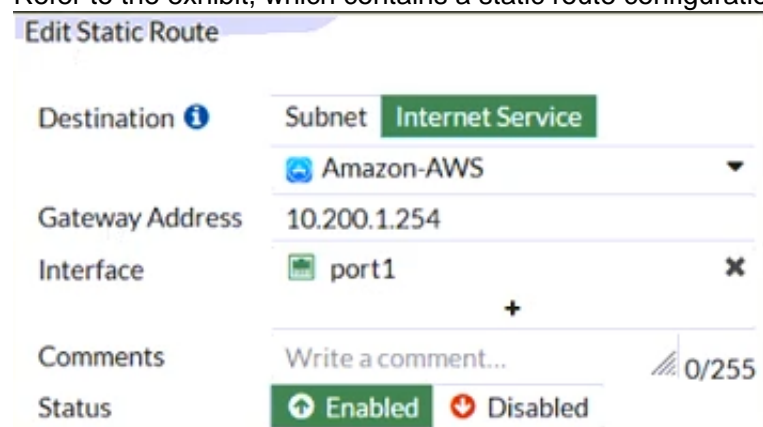
Based on the phase 2 configuration shown in the exhibit, what configuration change will bring phase 2 up?

- A. On HQ-FortiGate, enable Auto-negotiate.  
B. On Remote-FortiGate, set Seconds to 43200.  
C. On HQ-FortiGate, enable Diffie-Hellman Group 2.  
D. On HQ-FortiGate, set Encryption to AES256.

Answer: D

#### NEW QUESTION 15

Refer to the exhibit, which contains a static route configuration. An administrator created a static route for Amazon Web Services.



Which CLI command must the administrator use to view the route?

- A. get router info routing-table database  
B. diagnose firewall route list  
C. get internet-service route list  
D. get router info routing-table all

**Answer:** B

**Explanation:**

ISDB static route will not create entry directly in routing-table. Reference: <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for-Predefined-Internet/ta-p/1>

and here

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching-policy-route/ta-p/190640>

FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): "Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table." "FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command."

**NEW QUESTION 19**

Which two types of traffic are managed only by the management VDOM? (Choose two.)

- A. FortiGuard web filter queries
- B. PKI
- C. Traffic shaping
- D. DNS

**Answer:** AD

**NEW QUESTION 22**

Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate points the collector agent to use a remote LDAP server.
- B. FortiGate uses the AD server as the collector agent.
- C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- D. FortiGate queries AD by using the LDAP to retrieve user group information.

**Answer:** CD

**Explanation:**

Fortigate Infrastructure 7.0 Study Guide P.272-273 <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

**NEW QUESTION 23**

The IPS engine is used by which three security features? (Choose three.)

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

**Answer:** ABC

**Explanation:**

FortiGate Security 7.2 Study Guide (p.385): "The IPS engine is responsible for most of the features shown in this lesson: IPS and protocol decoders. It's also responsible for application control, flow-based antivirus protection, web filtering, and email filtering."

**NEW QUESTION 24**

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 27**

Refer to the exhibit.

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

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster. Which two statements are true? (Choose two.)

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

**Answer:** AD

**Explanation:**

\* 1. Override is disable by default - OK

\* 2. "If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the primary"

The QUESTION NO: here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide.

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disab>

**NEW QUESTION 30**

Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.

B. ADVPN is only supported with IKEv2.

C. Tunnels are negotiated dynamically between spokes.

D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

**Answer:** AC

**NEW QUESTION 33**

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:** D

**Explanation:**

FortiGate Security 7.2 Study Guide (p.15): "When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic."

When using FortiGuard servers for DNS, FortiOS defaults to using DNS over TLS (DoT) to secure the DNS traffic<sup>1</sup>. DNS over TLS is a protocol that encrypts and authenticates DNS queries and responses using the Transport Layer Security (TLS) protocol<sup>2</sup>. This prevents eavesdropping, tampering, and spoofing of DNS data by third parties.

The default FortiGuard DNS servers are 96.45.45.45 and 96.45.46.46, and they use the hostname globalsdns.fortinet.net<sup>1</sup>. The FortiGate verifies the server hostname using the server-hostname setting in the system dns configuration<sup>1</sup>.

**NEW QUESTION 34**

Which scanning technique on FortiGate can be enabled only on the CLI?

A. Heuristics scan

B. Trojan scan

C. Antivirus scan

D. Ransomware scan

**Answer:** A

**NEW QUESTION 36**

What are two characteristics of FortiGate HA cluster virtual IP addresses? (Choose two.)

A. Virtual IP addresses are used to distinguish between cluster members.

B. Heartbeat interfaces have virtual IP addresses that are manually assigned.

C. The primary device in the cluster is always assigned IP address 169.254.0.1.

D. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.

**Answer:** AD

**Explanation:**

Fortigate Infrastructure 7.2 Study Guide page 301 FortiGate Infrastructure 7.2 Study Guide (p.301):

"FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number."

"A change in the heartbeat IP addresses may happen when a FortiGate device joins or leaves the cluster." "The HA cluster uses the heartbeat IP addresses to distinguish the cluster members and synchronize data." <https://networkinterview.com/fortigate-ha-high-availability/>

**NEW QUESTION 37**

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

A. Application control can identity 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 identity web applications.

D. Application control does not display a replacement message for a blocked web application.

**Answer:** A

**Explanation:**

Application control is a feature that allows FortiGate to inspect and control the use of specific web applications on the network. When application control is enabled, FortiGate can identify child and parent applications, and can perform different actions on them based on the configuration.

### NEW QUESTION 38

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 43

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 44

Refer to the exhibit.



The screenshot shows the FortiGate SLA configuration page. The 'Name' field is 'SLA1'. The 'Protocol' section has 'Ping', 'HTTP', and 'DNS' buttons, with 'Ping' selected. The 'Server' section has two entries: '4.2.2.2' and '4.2.2.1', each with a delete icon. The 'Participants' section has a dropdown menu showing 'All SD-WAN Members' and a 'Specify' button. Below the dropdown, there are two entries: 'port1' and 'port2', each with a delete icon. At the bottom, there is a checkbox for 'Enable probe packets' which is currently unchecked.

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 46

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 47

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:** AC

#### Explanation:

The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:

FGCP elects the primary FortiGate device: In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block. FGCP uses a variety of factors, such as the device's priority, to determine which device should be the primary.

FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices. FGCP does not run over other types of links, such as data links.

#### NEW QUESTION 49

Refer to the exhibits.

Exhibit A Exhibit B

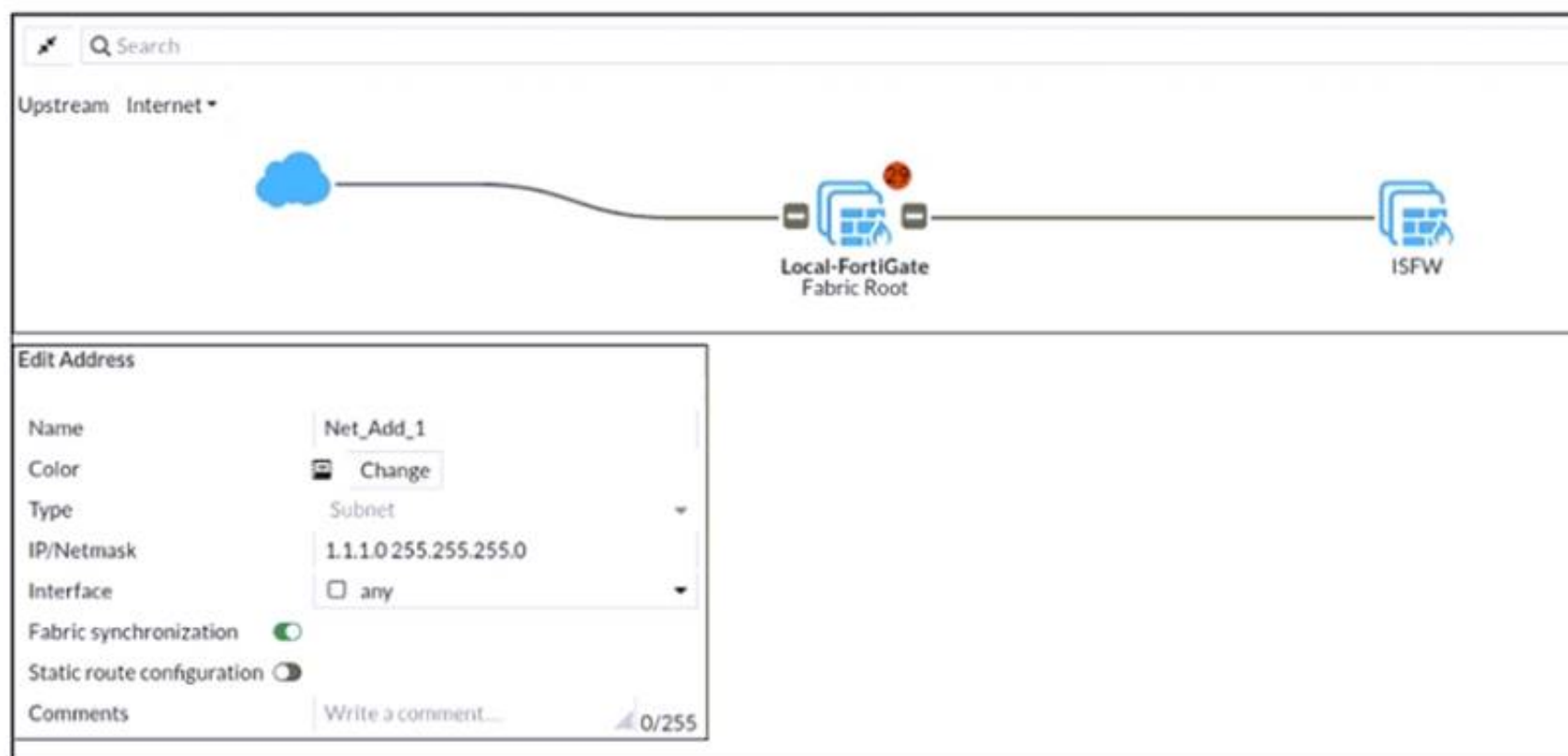


Exhibit A Exhibit B

<pre> Local-FortiGate # show full-configuration system csf config system csf     set status enable     set upstream ''     set upstream-port 8013     set group-name "fortinet"     set group-password ENC Y9ynT+64RpCTpVdgSmoQH242mYSIzNNzLNvgzMXjyN 9hSjIJE3KYJlo3XxygldvNxPI8T5xctBUSzy7rgIcHcA/qHrByXSXfPEeHC6ufkqlPJr W6GypwDUB5O3VFgPbASFYteQesmwoJtGe84BLqa+hUcgunLD1z/97sBp+PLt5nrA==     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 default     set saml-configuration-sync default         </pre>	<pre> ISFW # show full-configuration system csf config system csf     set status enable     set upstream "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 local end ISFW #         </pre>
--	--

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 ISFW (downstream) to set configuration-sync local.
- B. Change the csf setting on ISFW (downstream) to set authorization-request-type certificate.
- C. Change the csf setting on both devices to set downstream-access enable.
- D. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.

Answer: C

### NEW QUESTION 50

An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must an administrator do to achieve this objective?

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

Answer: B

### NEW QUESTION 52

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 54

Which feature in the Security Fabric takes one or more actions based on event triggers?

- A. Fabric Connectors
- B. Automation Stitches
- C. Security Rating
- D. Logical Topology

Answer: B

#### NEW QUESTION 55

Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

- A. The next-hop IP address is unreachable.
- B. It failed the RPF check .
- C. It matched an explicitly configured firewall policy with the action DENY.
- D. It matched the default implicit firewall policy.

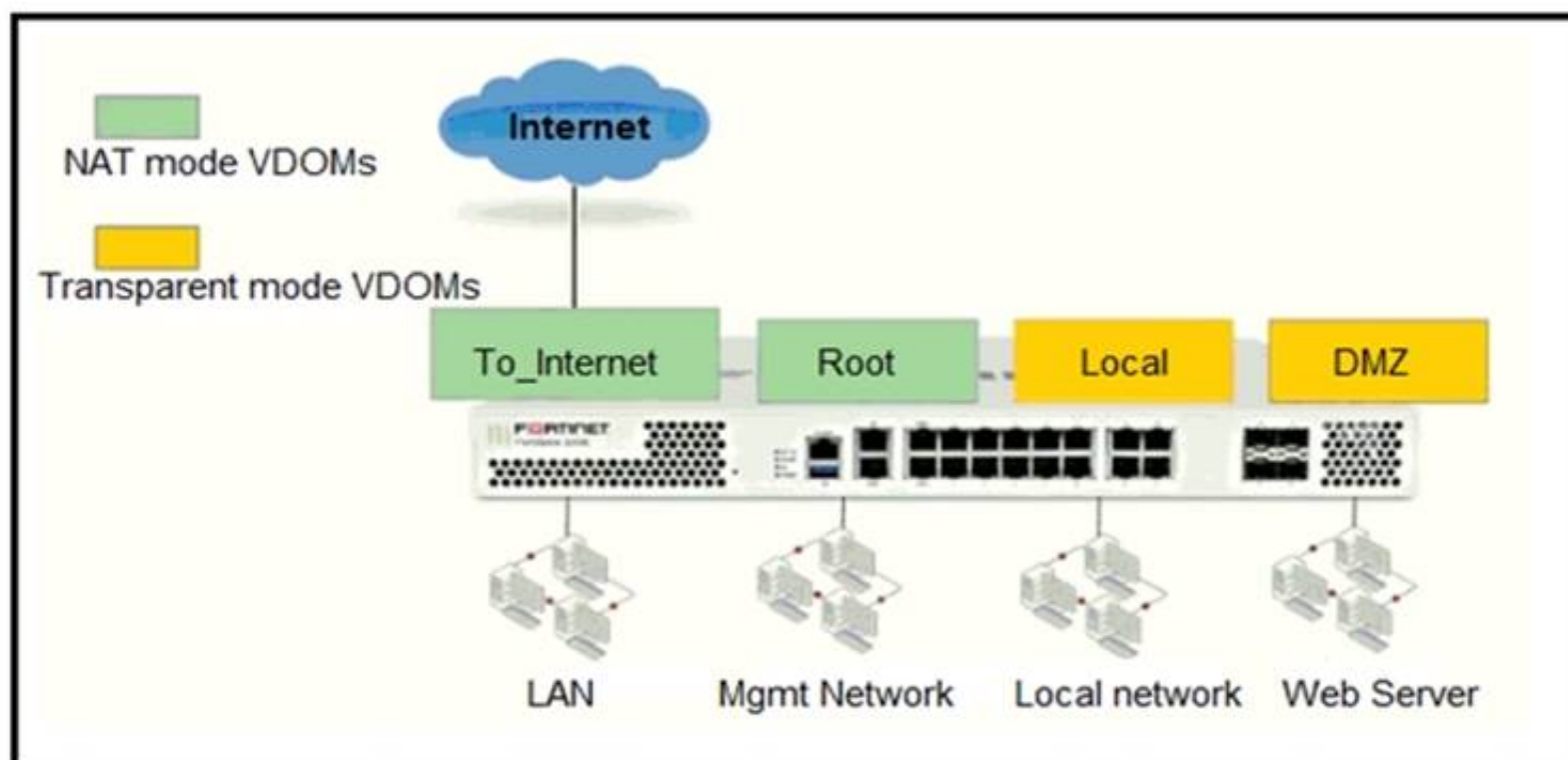
Answer: D

#### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=13900> <https://www.fortinetguru.com/2016/03/what-is-policy-id-0-and-why-lot-of-denied-traffic-on-this-policy/>

#### NEW QUESTION 59

Refer to the exhibit.



The Root and To\_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode. The Root VDOM is the management VDOM. The To\_Internet VDOM allows LAN users to access the internet. The To\_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem . With this configuration, which statement is true?

- A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
- B. A static route is required on the To\_Internet VDOM to allow LAN users to access the internet.
- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
- D. Inter-VDOM links are not required between the Root and To\_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: A

#### NEW QUESTION 64

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

**Answer:** BC

**Explanation:**

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-identify-Inactive-Routes-in-the-Routing/ta-p>

#### NEW QUESTION 67

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

- A. The interface has been configured for one-arm sniffer.
- B. The interface is a member of a virtual wire pair.
- C. The operation mode is transparent.
- D. The interface is a member of a zone.
- E. Captive portal is enabled in the interface.

**Answer:** ABC

**Explanation:**

[https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top\\_VirtualWirePair.htm](https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm)

#### NEW QUESTION 69

Which statement regarding the firewall policy authentication timeout is true?

- A. It is an idle timeout
- B. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
- C. It is a hard timeout
- D. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
- E. It is an idle timeout
- F. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.
- G. It is a hard timeout
- H. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

**Answer:** A

#### NEW QUESTION 70

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 74

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface. In this scenario, which statement about VLAN IDs is true?

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



D. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in different subnets.

**Answer:** CD

#### NEW QUESTION 78

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

- A. IP tool references must be removed from existing firewall policies before enabling central NAT .
- B. Central NAT can be enabled or disabled from the CLI only.
- C. Source NAT, using central NAT, requires at least one central SNAT policy.
- D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

**Answer:** AB

#### NEW QUESTION 83

Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

- A. FortiGuard web filter cache
- B. FortiGate hostname
- C. NTP
- D. DNS

**Answer:** CD

#### Explanation:

In the 7.2 Infrastructure Guide (page 306) the list of configuration settings that are NOT synchronized includes both 'FortiGate host name' and 'Cache'

#### NEW QUESTION 86

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy. Which two other security profiles can you apply to the security policy? (Choose two.)

- A. Antivirus scanning
- B. File filter
- C. DNS filter
- D. Intrusion prevention

**Answer:** AD

#### NEW QUESTION 89

An administrator wants to configure timeouts for users. Regardless of the userTMs behavior, the timer should start as soon as the user authenticates and expire after the configured value.

Which timeout option should be configured on FortiGate?

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

**Answer:** E

#### Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-TipExplanation:-of-auth-timeout-types-for-Firewall/ta-p/>

#### NEW QUESTION 94

Which statement is correct regarding the security fabric?

- A. FortiManager is one of the required member devices.
- B. FortiGate devices must be operating in NAT mode.
- C. A minimum of two Fortinet devices is required.
- D. FortiGate Cloud cannot be used for logging purposes.

**Answer:** B

#### Explanation:

FortiGate Security 7.2 Study Guide (p.428): "You must have a minimum of two FortiGate devices at the core of the Security Fabric, plus one FortiAnalyzer or cloud logging solution. FortiAnalyzer Cloud or FortiGate Cloud can act as the cloud logging solution. The FortiGate devices must be running in NAT mode."

#### NEW QUESTION 98

Refer to the exhibit.

Username	Administrator	Change Password
Type	<div>Local User</div> <div>Match a user on a remote server group</div> <div>Match all users in a remote server group</div> <div>Use public key infrastructure (PKI) group</div>	
Comments	Write a comment... 0/255	
Administrator Profile	prof_admin	
Email Address	admin@xyz.com	
<input type="checkbox"/> SMS		
<input type="checkbox"/> Two-factor Authentication		
<input type="checkbox"/> Restrict login to trusted hosts		
<input type="checkbox"/> Restrict admin to guest account provisioning only		

The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?

- A. Change password
- B. Enable restrict access to trusted hosts
- C. Change Administrator profile
- D. Enable two-factor authentication

Answer: C

#### NEW QUESTION 102

Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

- A. Log downloads from the GUI are limited to the current filter view
- B. Log backups from the CLI cannot be restored to another FortiGate
- C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
- D. Log downloads from the GUI are stored as LZ4 compressed files.

Answer: AB

#### NEW QUESTION 103

Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

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

Answer: CD

#### Explanation:

https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf  
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883

NEW QUESTION 105  
Refer to the exhibit.

Exhibit A   Exhibit B

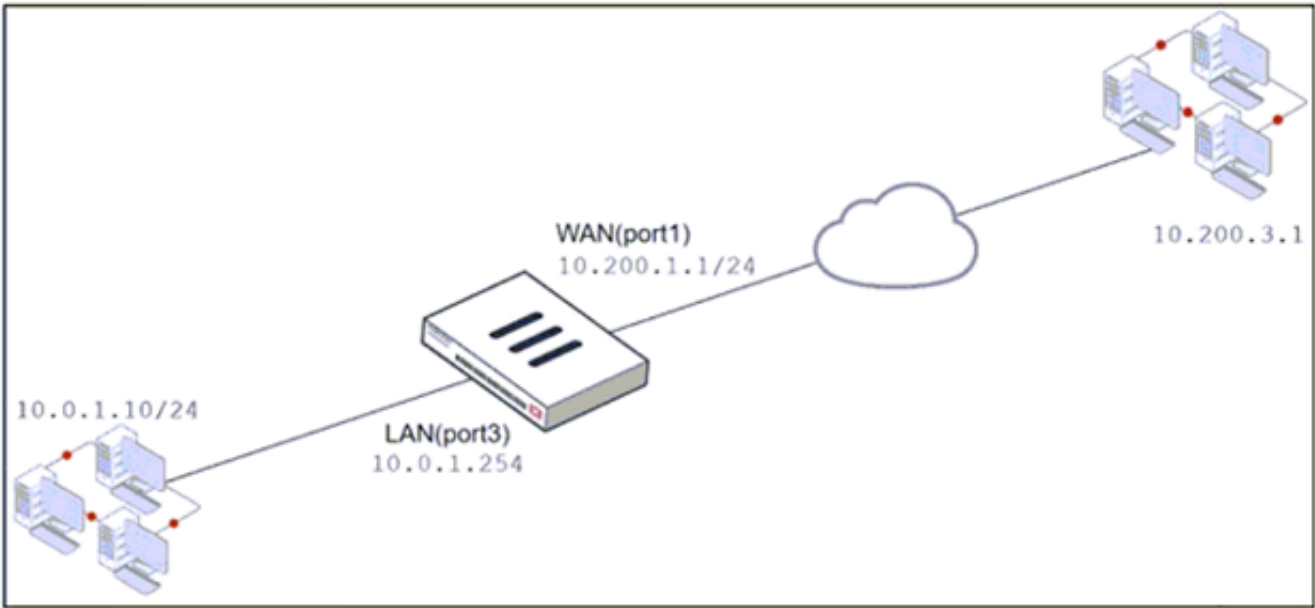


Exhibit A   Exhibit B

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... 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: Write a comment... 0/255

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: ☒

The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies 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. The first firewall policy has NAT enabled using IP Pool. The second firewall policy is configured with a VIP as the destination address. Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0. 1. 10?

- A. 10.200. 1. 1
- B. 10.200.3. 1
- C. 10.200. 1. 100
- D. 10.200. 1. 10

Answer: C

Explanation:

Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.

NEW QUESTION 107

Which statement about video filtering on FortiGate is true?

- A. Full SSL Inspection is not required.
- B. It is available only on a proxy-based firewall policy.
- C. It inspects video files hosted on file sharing services.
- D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Answer: B

#### NEW QUESTION 108

Which statement about video filtering on FortiGate is true?

- A. Video filtering FortiGuard categories are based on web filter FortiGuard categories.
- B. It does not require a separate FortiGuard license.
- C. Full SSL inspection is not required.
- D. its available only on a proxy-based firewall policy.

Answer: D

#### Explanation:

FortiGate Security 7.2 Study Guide (p.279): "To apply the video filter profile, proxy-based firewall policies currently allow you to enable the video filter profile. You must enable full SSL inspection on the firewall policy."

<https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/860867/filtering-based-on-fortiguard-cat>

#### NEW QUESTION 111

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 112

Refer to the exhibit.



Which contains a network diagram and routing table output. The Student is unable to access Webserver.

What is the cause of the problem and what is the solution for the problem?

- A. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
- B. The first reply packet for Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
- C. The first reply packet for Student failed the RPF check .This issue can be resolved by adding a static route to 203.0. 114.24/32 through port3.
- D. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 203.0. 114.24/32 through port3.

Answer: D

#### NEW QUESTION 116

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
orgin->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 117**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4\_FGT-7.0 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-7.0 Product From:

[https://www.2passeasy.com/dumps/NSE4\\_FGT-7.0/](https://www.2passeasy.com/dumps/NSE4_FGT-7.0/)

## Money Back Guarantee

### NSE4\_FGT-7.0 Practice Exam Features:

- \* NSE4\_FGT-7.0 Questions and Answers Updated Frequently
- \* NSE4\_FGT-7.0 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE4\_FGT-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE4\_FGT-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year