
# 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

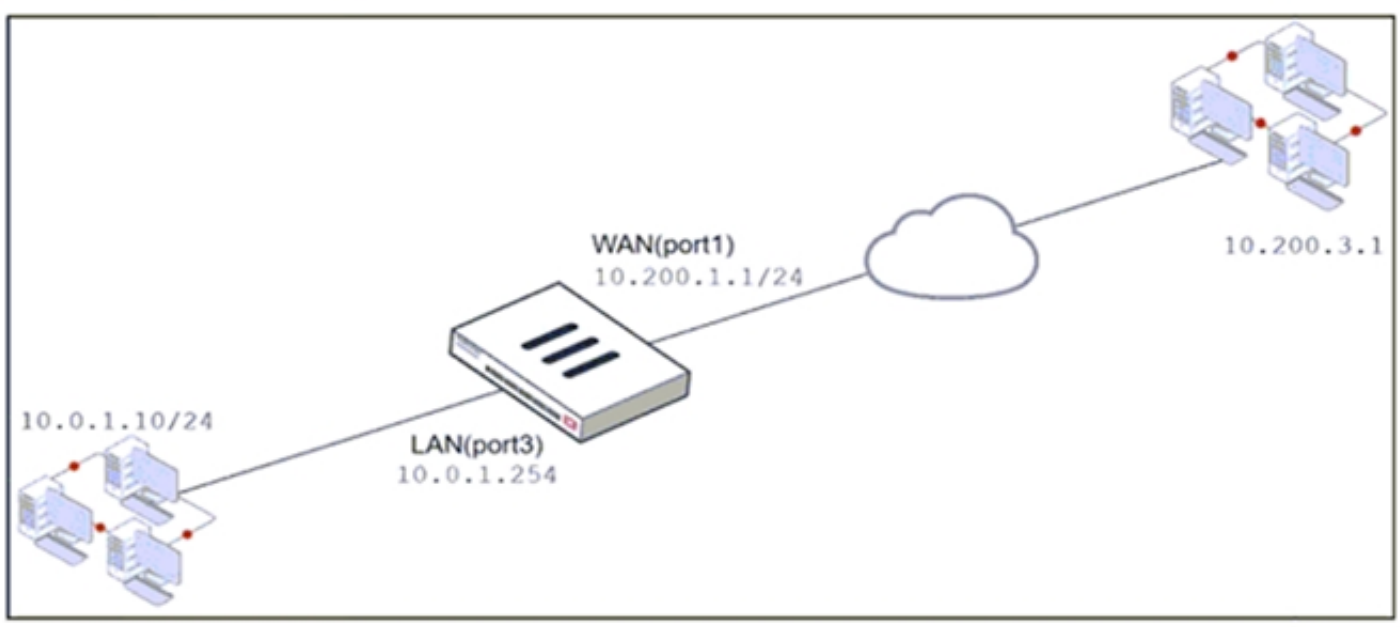



Exhibit A Exhibit B

| 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**
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**
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 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**
What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

A. FortiGate uses fewer resources.
B. FortiGate performs a more exhaustive inspection on traffic.
C. FortiGate adds less latency to traffic.
D. FortiGate allocates two sessions per connection.

**Answer:** AC

**NEW QUESTION 6**
Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

A. The client FortiGate requires a manually added route to remote subnets.
B. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
C. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.
D. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN.

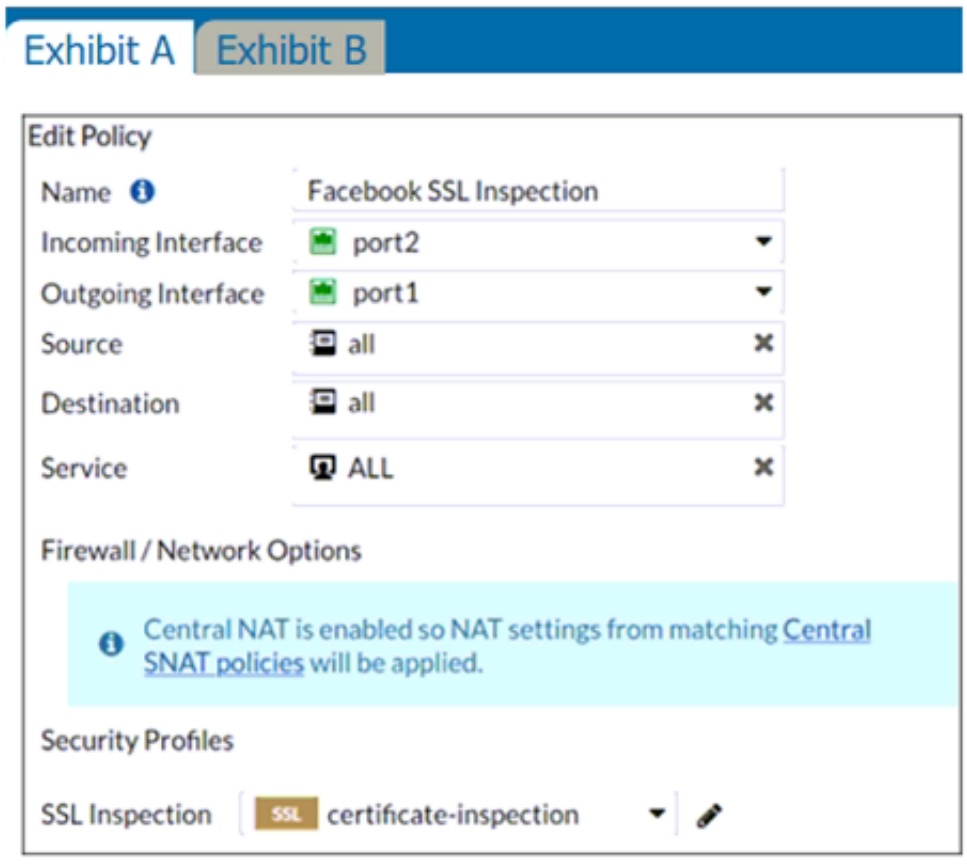
**Answer:** BC

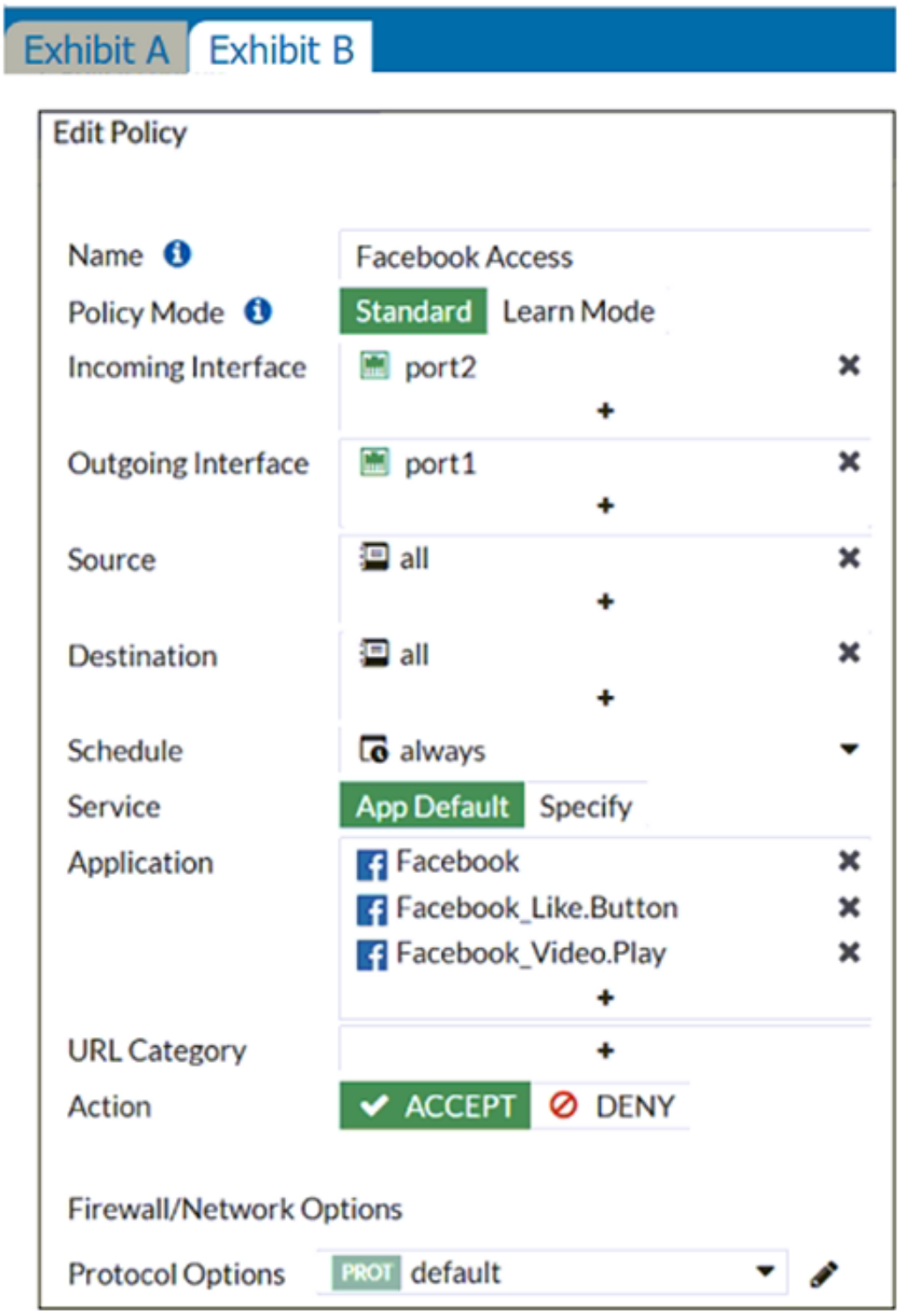
**NEW QUESTION 7**
FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.
In this scenario, what are two requirements for the VLAN ID? (Choose two.)

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

**Answer:** CD

**NEW QUESTION 8**
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.




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 9**
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

**NEW QUESTION 10**
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 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 12**
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 16**
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 20**
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 24**
Which two statements explain antivirus scanning modes? (Choose two.)

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

**Answer:** BC

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

**NEW QUESTION 29**
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**
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 34**
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

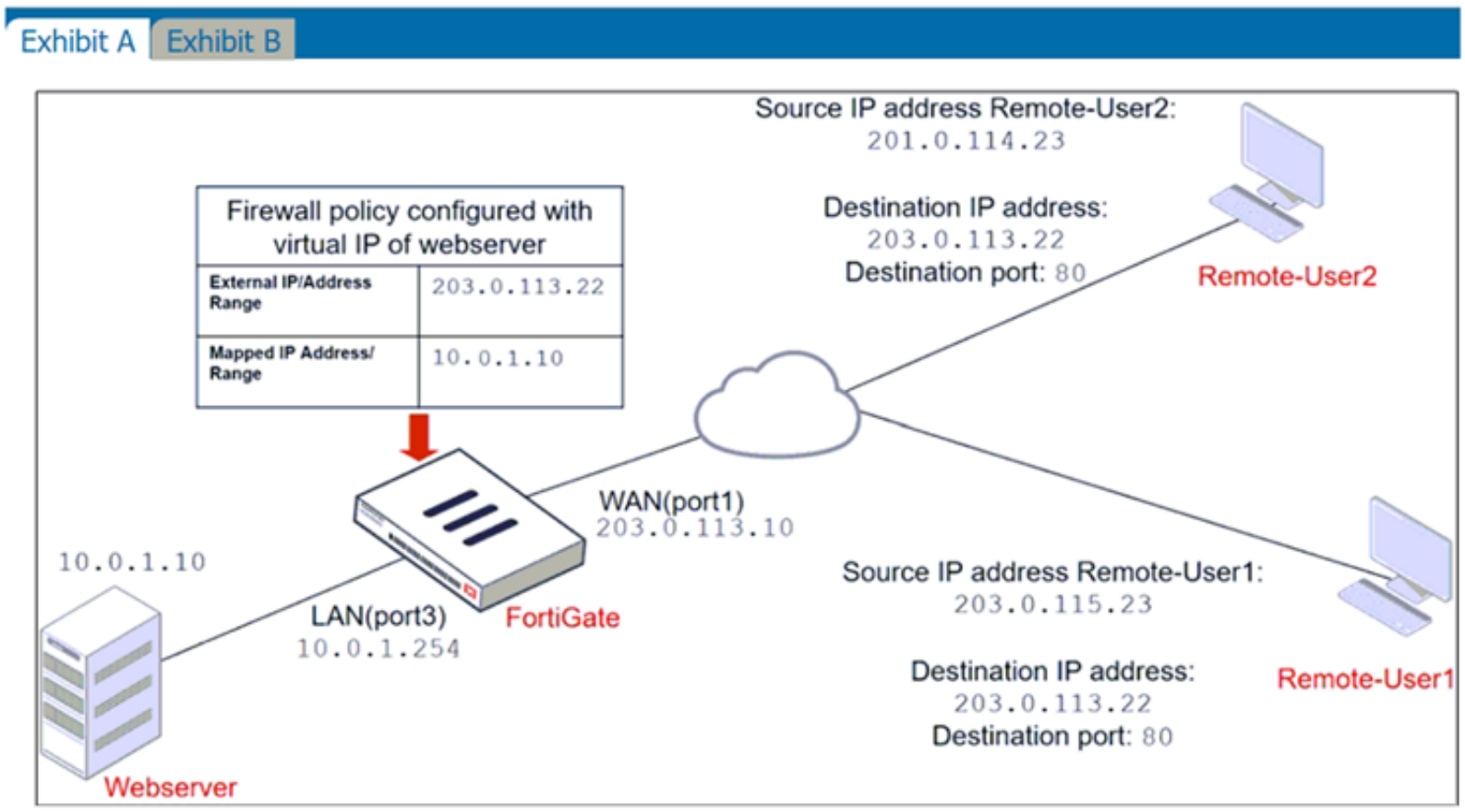
**NEW QUESTION 35**
Which two statements are correct about a software switch on FortiGate? (Choose two.)

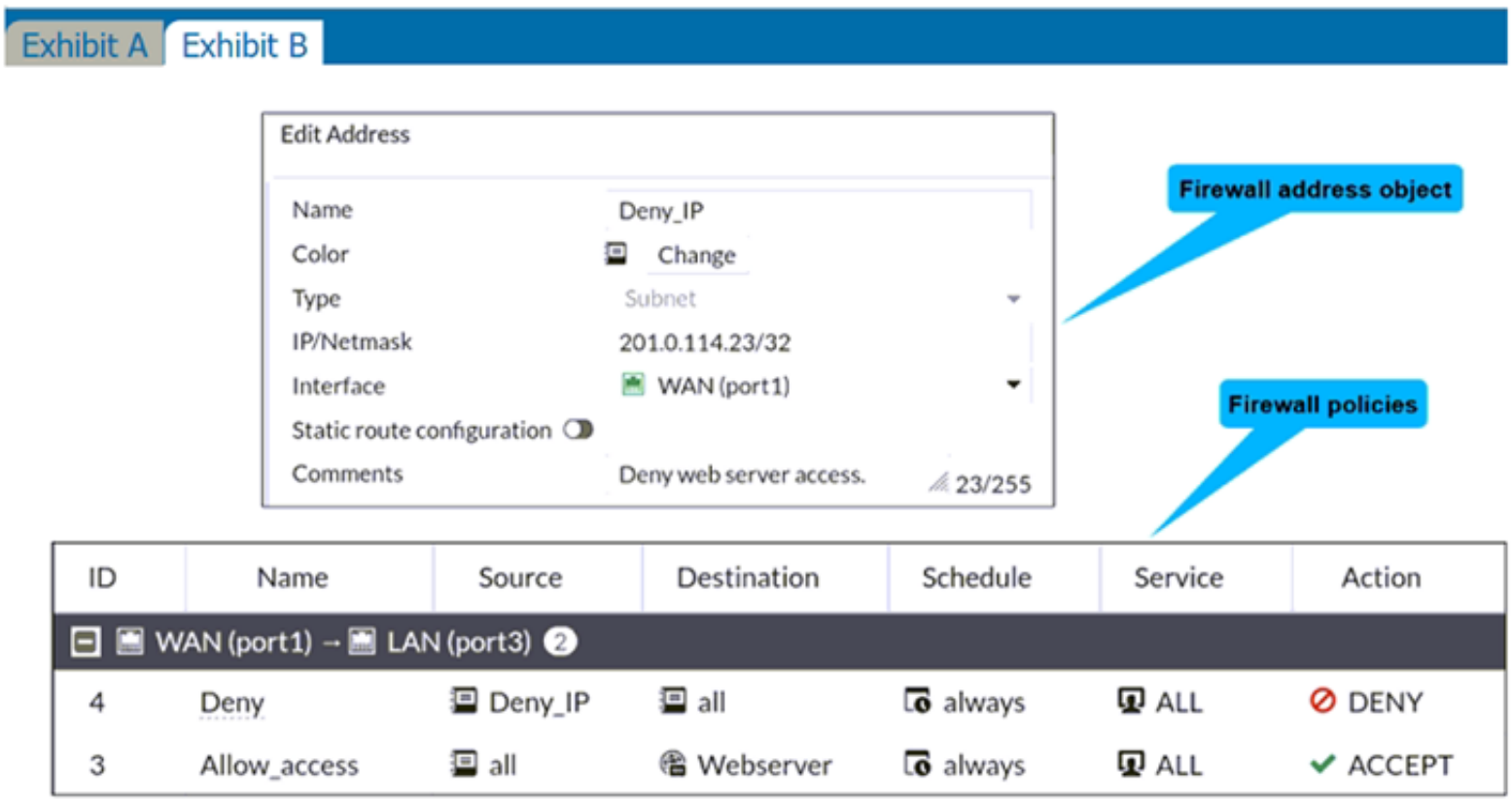
A. It can be configured only when FortiGate is operating in NAT mode
B. Can act as a Layer 2 switch as well as a Layer 3 router
C. All interfaces in the software switch share the same IP address
D. It can group only physical interfaces

**Answer:** AC

**NEW QUESTION 39**

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.




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 40**
Refer to the exhibit.


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 44**
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 45**
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 overTLS.

**Answer:** B

**NEW QUESTION 49**
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 52**
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 53**
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 57**
Refer to the exhibits.
Exhibit A.

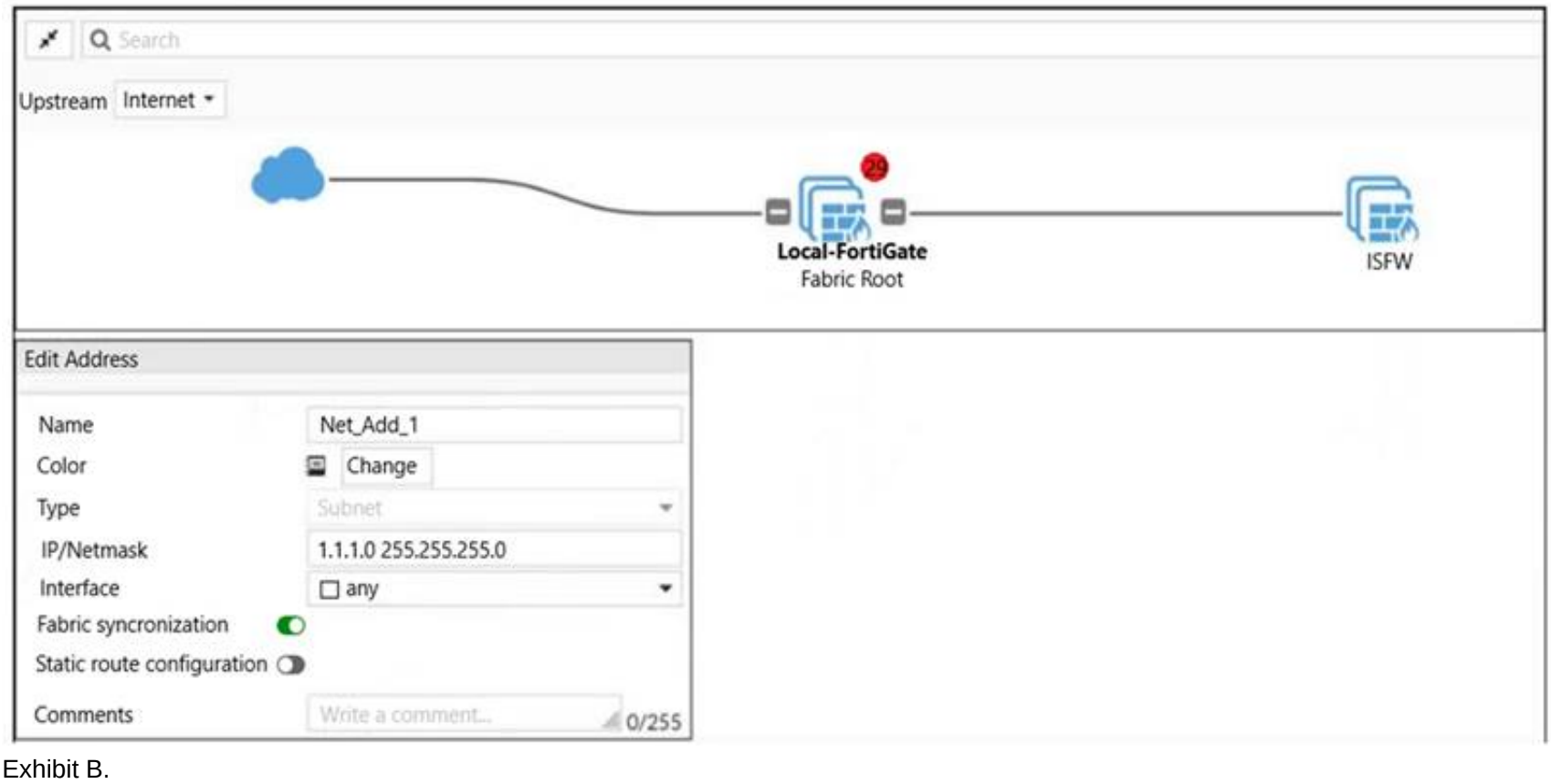



Exhibit B.

```
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 59**
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 60**
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 65**
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

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

**Answer:** A

**NEW QUESTION 68**
.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons 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