Free Questions for NSE4_FGT-7.2 by certscare

Shared by Lott on 29-01-2024

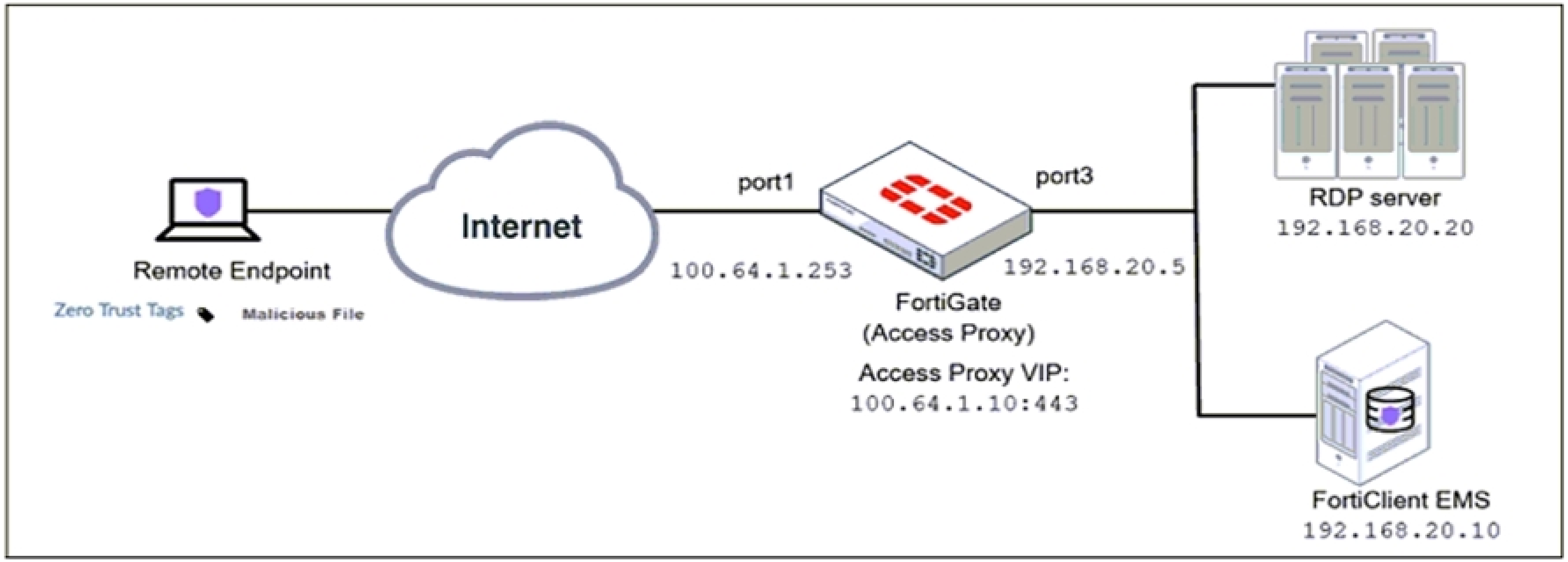
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



Based on the ZTNA tag, the security posture of the remote endpoint has changed.

What will happen to endpoint active ZTNA sessions?

Options:

A- They will be re-evaluated to match the endpoint policy.

B- They will be re-evaluated to match the firewall policy.

C- They will be re-evaluated to match the ZTNA policy.

D- They will be re-evaluated to match the security policy.

Answer:

C

Explanation:

https://docs.fortinet.com/document/fortigate/7.0.0/new-features/580880/posture-check-verification-for-active-ztna-proxy-session-7-0-2

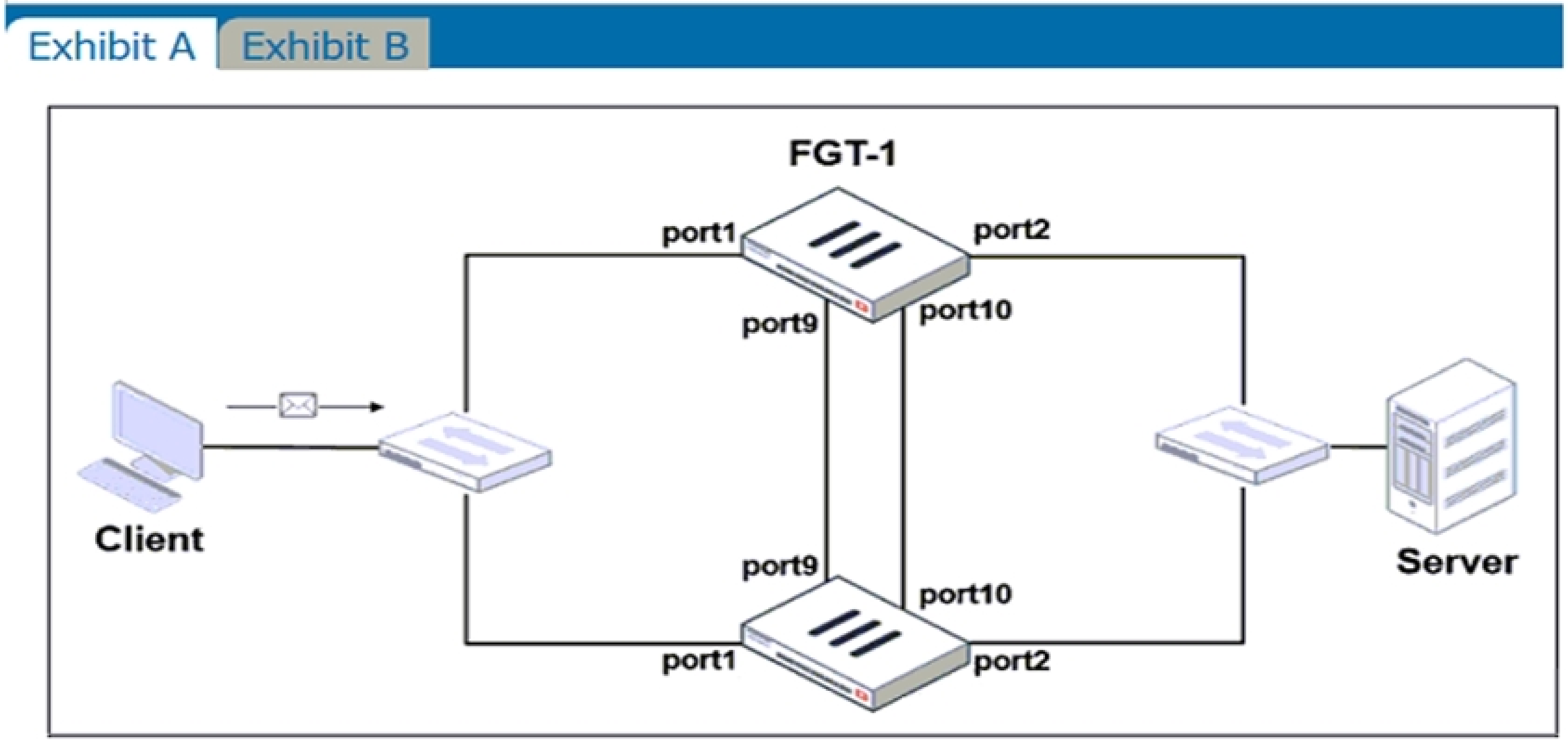
FortiGate Infrastructure 7.2 Study Guide (p.182): 'Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy.'

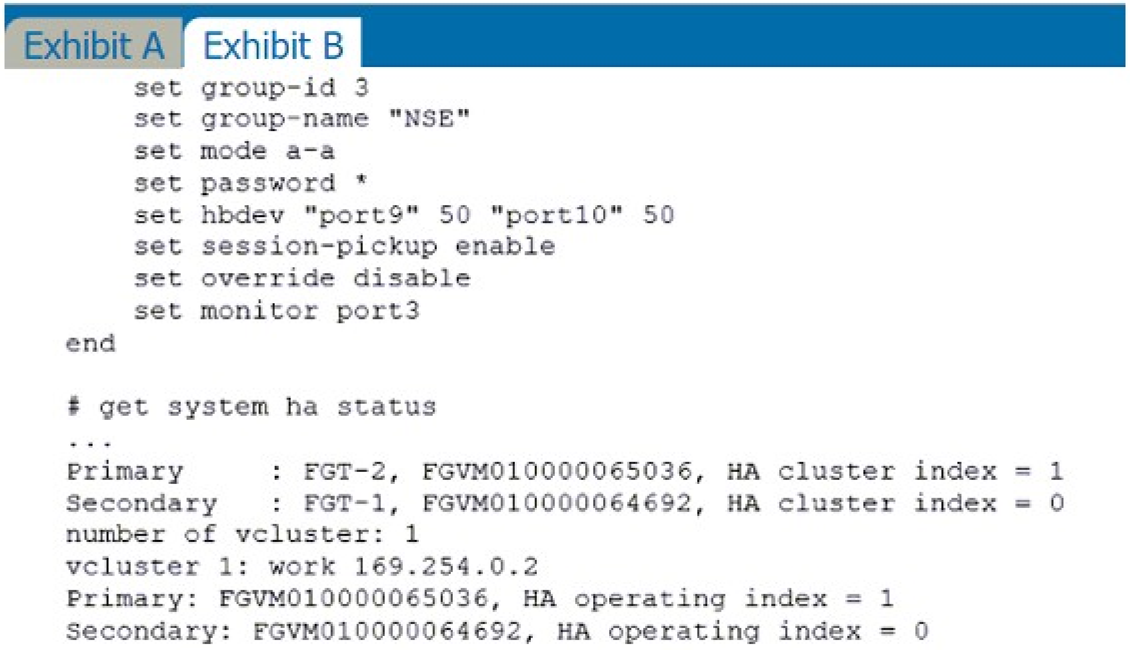
Question 2

Question Type: MultipleChoice

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.





```
        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.)

Options:

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:

A, D

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.'

Question 3

Question Type: MultipleChoice

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

Options:

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.

Question 4

Question Type: MultipleChoice

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

Options:

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

Explanation:

The SSL VPN idle-timeout setting determines how long an SSL VPN session can be inactive before it is terminated. When an SSL VPN session becomes inactive (for example, if the user closes the VPN client or disconnects from the network), the session timer begins to count down. If the timer reaches the idle-timeout value before the user reconnects or sends any new traffic, the session will be terminated and the associated resources (such as VPN tunnels and virtual interfaces) will be deleted.

Question 5

Question Type: MultipleChoice

What are two functions of ZTNA? (Choose two.)

Options:

A- ZTNA manages access through the client only.

B- ZTNA manages access for remote users only.

C- ZTNA provides a security posture check.

D- ZTNA provides role-based access.

Answer:

C, D

Explanation:

ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of 'never trust, always verify,' which means that all access to network resources is subject to strict verification and authentication.

Two functions of ZTNA are:

ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the device's software and hardware configurations, security settings, and the presence of malware.

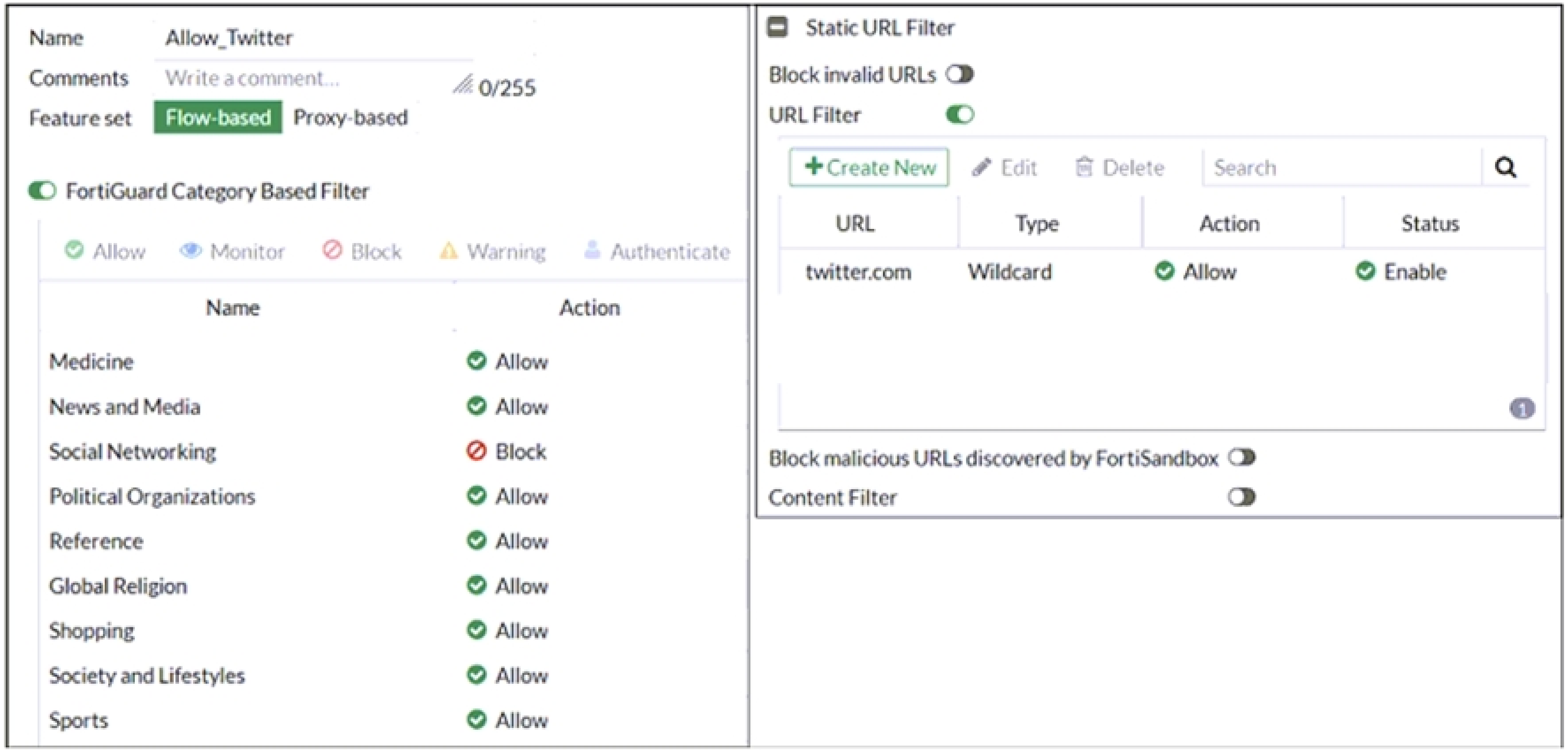
ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data breaches.

Question 6

Question Type: MultipleChoice

Refer to exhibit.

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



Name Allow_Twitter

Comments Write a comment... 0/255

Feature set Flow-based Proxy-based

FortiGuard Category Based Filter

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

Static URL Filter

Block invalid URLs

URL Filter

URL	Type	Action	Status
twitter.com	Wildcard	✓ Allow	✓ Enable

Block malicious URLs discovered by FortiSandbox

Content Filter

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

Options:

A- On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking

B- On the Static URL Filter configuration, set Type to Simple

C- On the Static URL Filter configuration, set Action to Exempt.

D- On the Static URL Filter configuration, set Action to Monitor.

Answer:

C

Explanation:

Based on the exhibit, the administrator has configured the FortiGuard Category Based Filter to block access to all social networking sites, and has also configured a Static URL Filter to block access to twitter.com. As a result, users are being redirected to a block page when they try to access twitter.com. To allow users to access twitter.com while blocking all other social networking sites, the administrator can make the following configuration change: On the Static URL Filter configuration, set Action to Exempt: By setting the Action to Exempt, the administrator can override the block on twitter.com that was specified in the FortiGuard Category Based Filter. This will allow users to access twitter.com, while all other social networking sites will still be blocked.

Question 7

Question Type: **MultipleChoice**

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

Options:

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:

A, C

Explanation:

Flow-based inspection is a type of traffic inspection that is used by some firewall devices, including FortiGate, to analyze network traffic. It is designed to be more efficient and less resource-intensive than proxy-based inspection, and it offers several benefits over this approach.

Two benefits of flow-based inspection compared to proxy-based inspection are:

FortiGate uses fewer resources: Flow-based inspection uses fewer resources than proxy-based inspection, which can help to improve the performance of the firewall device and reduce the impact on overall system performance.

FortiGate adds less latency to traffic: Flow-based inspection adds less latency to traffic than proxy-based inspection, which can be important for real-time applications or other types of traffic that require low latency.

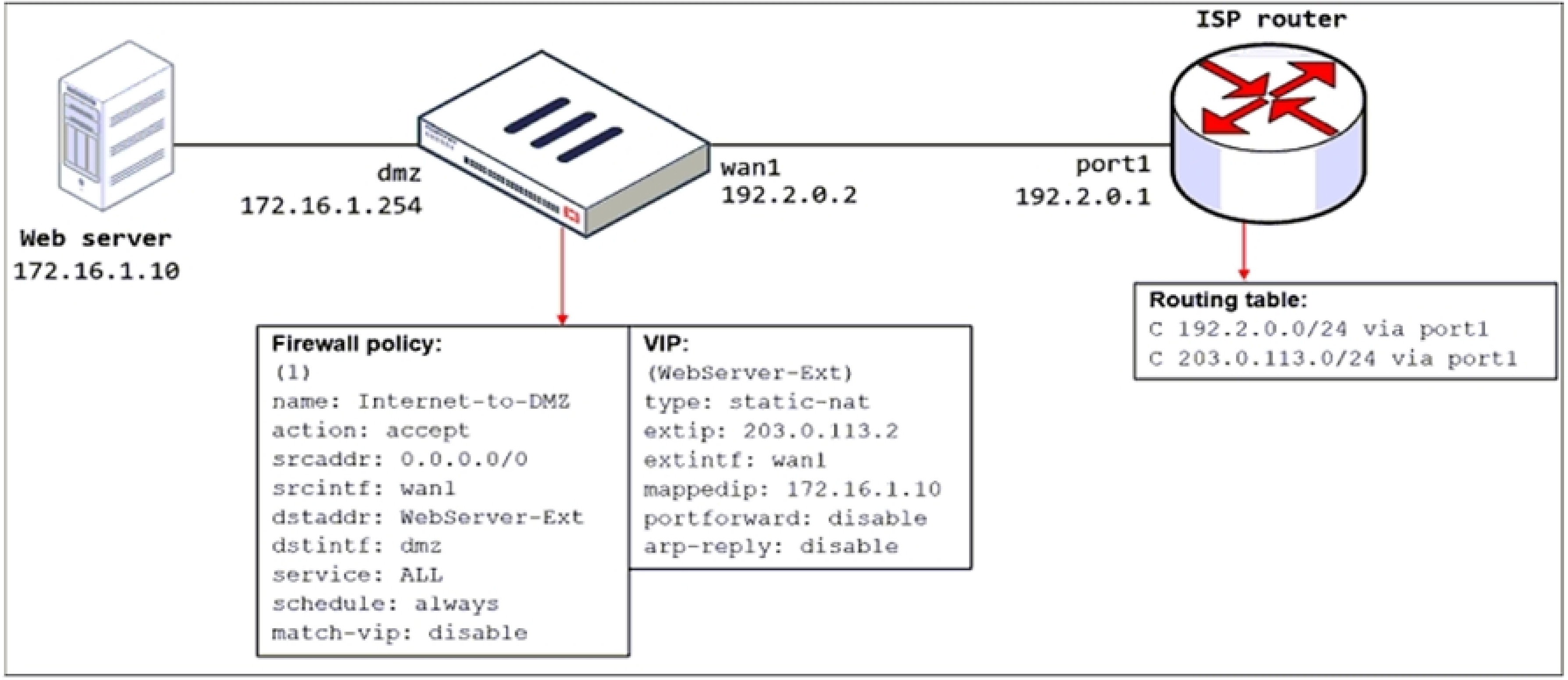
Question 8

Question Type: MultipleChoice

Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.

When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.



Firewall policy:

```
(1)
name: Internet-to-DMZ
action: accept
srcaddr: 0.0.0.0/0
srcintf: wan1
dstaddr: WebServer-Ext
dstintf: dmz
service: ALL
schedule: always
match-vip: disable
```

VIP:

```
(WebServer-Ext)
type: static-nat
extip: 203.0.113.2
extintf: wan1
mappedip: 172.16.1.10
portforward: disable
arp-reply: disable
```

Routing table:

```
C 192.2.0.0/24 via port1
C 203.0.113.0/24 via port1
```

Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

Options:

A- Configure a loopback interface with address 203.0.113.2/32.

B- In the VIP configuration, enable arp-reply.

C- Enable port forwarding on the server to map the external service port to the internal service port.

D- In the firewall policy configuration, enable match-vip.

Answer:

B

Explanation:

FortiGate Security 7.2 Study Guide (p.115): 'Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it's a best practice to keep ARP reply enabled.'

Question 9

Question Type: **MultipleChoice**

Which statement correctly describes the use of reliable logging on FortiGate?

Options:

A- Reliable logging is enabled by default in all configuration scenarios.

B- Reliable logging is required to encrypt the transmission of logs.

C- Reliable logging can be configured only using the CLI.

D- Reliable logging prevents the loss of logs when the local disk is full.

Answer:

B

Explanation:

FortiGate Security 7.2 Study Guide (p.192): 'if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can choose the level of SSL protection used by configuring the enc-algorithm setting on the CLI.'

Question 10

Question Type: **MultipleChoice**

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?

Options:

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:

C, D

Question 11

Question Type: **MultipleChoice**

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.

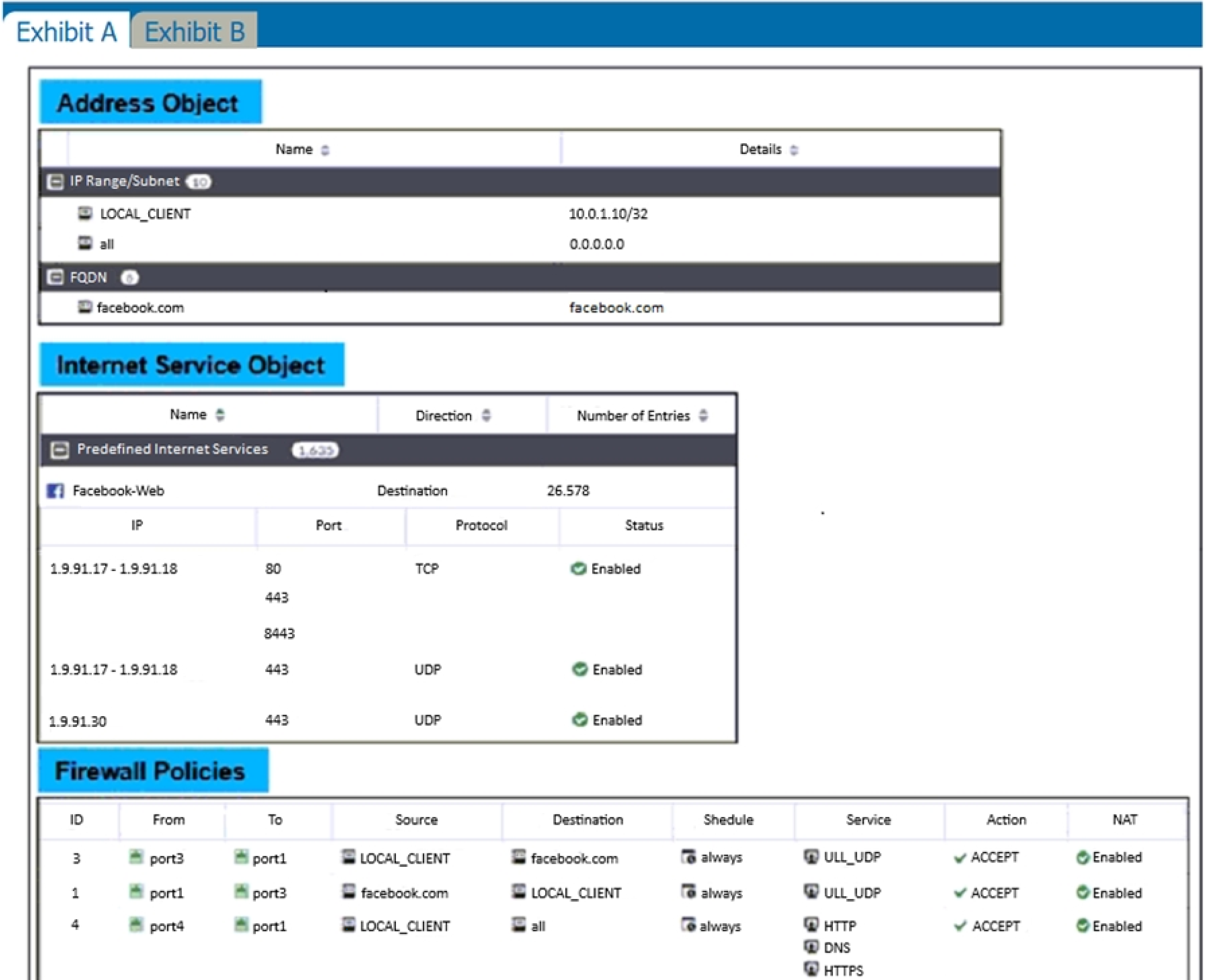


Exhibit A | Exhibit B

Address Object

Name	Details
IP Range/Subnet 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN 6	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services 1,635		
Facebook-Web	Destination	26.578

IP	Port	Protocol	Status
1.9.91.17 - 1.9.91.18	80 443 8443	TCP	✓ Enabled
1.9.91.17 - 1.9.91.18	443	UDP	✓ Enabled
1.9.91.30	443	UDP	✓ Enabled

Firewall Policies

ID	From	To	Source	Destination	Shedule	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

Which policy will be highlighted, based on the input criteria?

Options:

A- Policy with ID 4.

B- Policy with ID 5.

C- Policies with ID 2 and 3.

D- Policy with ID 4.

Answer:

B

Explanation:

We are looking for a policy that will allow or deny traffic from the source interface Port3 and source IP address 10.1.1.10 (LOCAL_CLIENT) to facebook.com TCP port 443 (HTTPS). There are only two policies that will match this traffic, policy ID 2 and 5. In FortiGate, firewall policies are evaluated from top to bottom. This means that the first policy that matches the traffic is applied, and subsequent policies are not evaluated. Based on the Policy Lookup criteria, Policy ID 5 will be highlighted

Question 12

Question Type: **MultipleChoice**

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

Options:

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