

NSE4_FGT-7.2^{Q&As}

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse4_fgt-7-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

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

Comments 0/255

Feature set **Flow-based** Proxy-based

FortiGuard Category Based Filter

Allow Monitor Block Warning Authenticate

Name	Action
Medicine	<input checked="" type="checkbox"/> Allow
News and Media	<input checked="" type="checkbox"/> Allow
Social Networking	<input type="checkbox"/> Block
Political Organizations	<input checked="" type="checkbox"/> Allow
Reference	<input checked="" type="checkbox"/> Allow
Global Religion	<input checked="" type="checkbox"/> Allow
Shopping	<input checked="" type="checkbox"/> Allow
Society and Lifestyles	<input checked="" type="checkbox"/> Allow
Sports	<input checked="" type="checkbox"/> Allow

Static URL Filter

Block invalid URLs

URL Filter

URL	Type	Action	Status
twitter.com	Wildcard	<input checked="" type="checkbox"/> Allow	<input checked="" type="checkbox"/> 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?

- 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.

Correct Answer: C

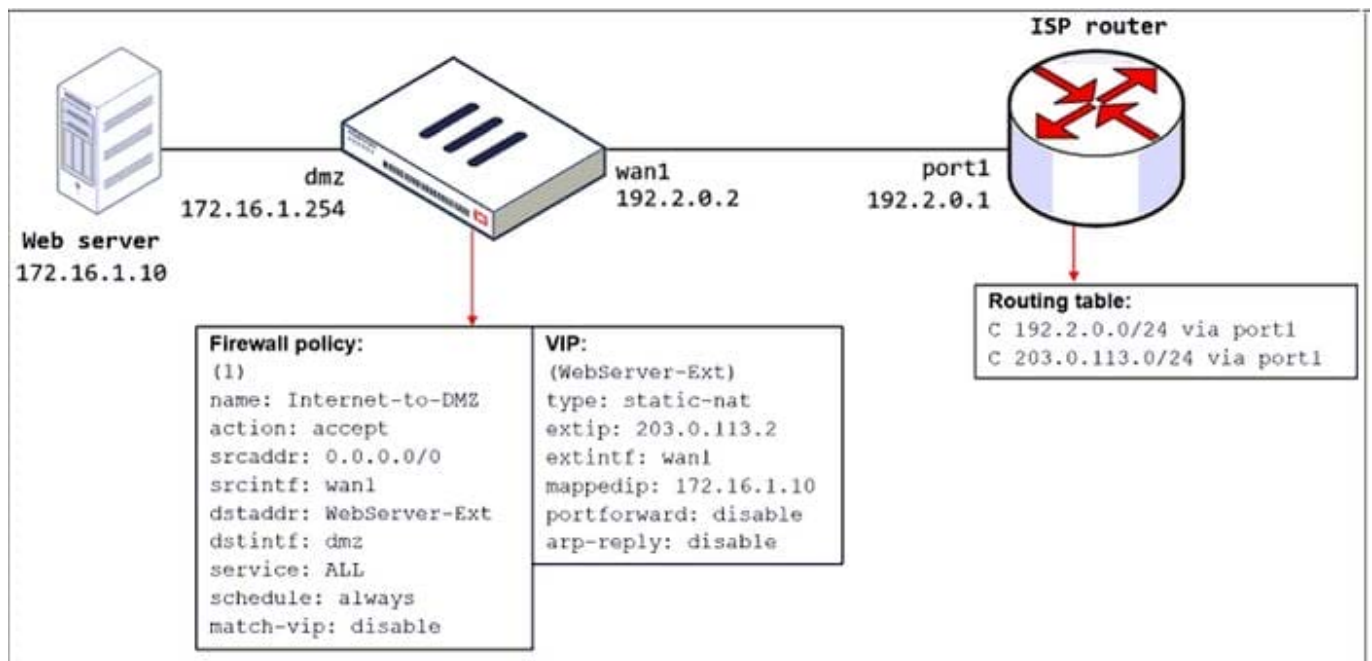
Reference: <https://fortinet77.rssing.com/chan-56127603/article113.html> Based on the exhibit, the administrator has configured the FortiGuard Category Based Filter to block access to all social networking sites, and has also configured a Static URL Filter to block access to twitter.com. As a result, 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 2

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.



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

- 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.

Correct Answer: B

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 3

Examine this FortiGate configuration: How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

```
config authentication setting
    set active-auth-scheme SCHEME1
end
config authentication rule
    edit WebProxyRule
        set srcaddr 10.0.1.0/24
        set active-auth-method SCHEME2
    next
end
```

- A. It always authorizes the traffic without requiring authentication.
- B. It drops the traffic.
- C. It authenticates the traffic using the authentication scheme SCHEME2.
- D. It authenticates the traffic using the authentication scheme SCHEME1.

Correct Answer: D

"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

QUESTION 4

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.

The administrator disabled the WebServer firewall policy.

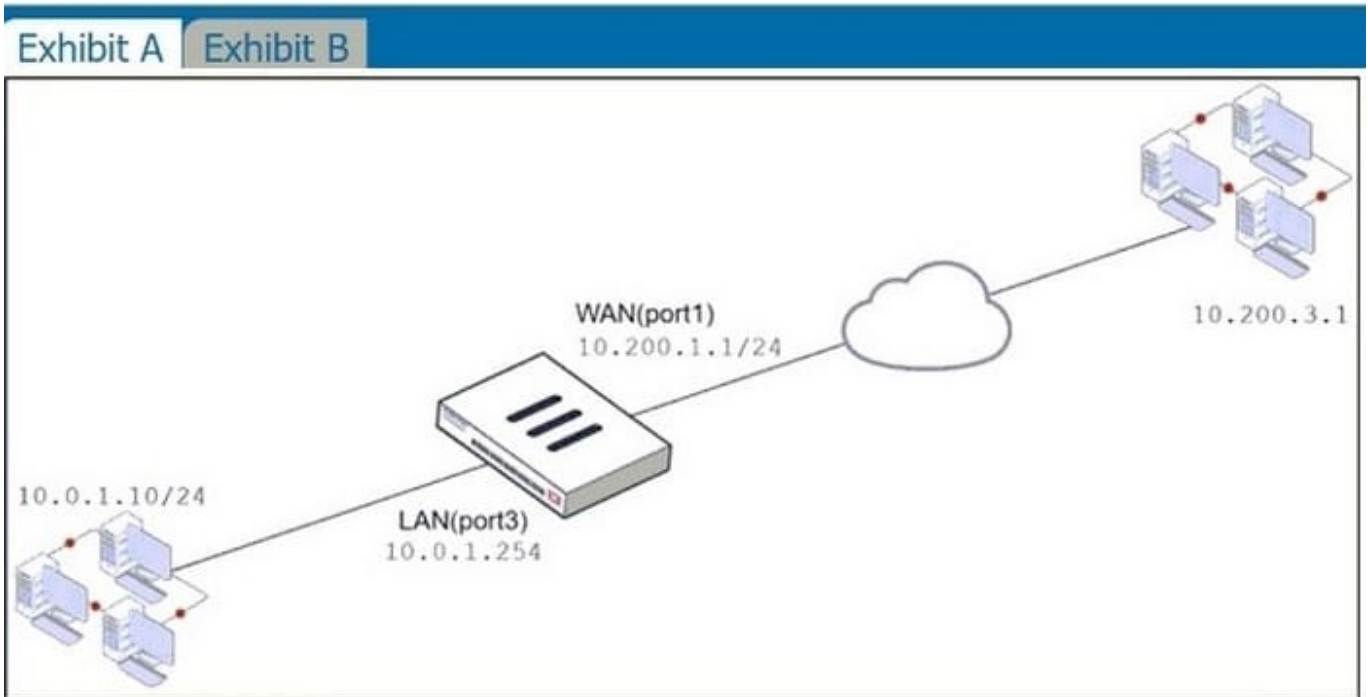


Exhibit A Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	ACCEPT	Enabled
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: 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

Which IP address will be used to source NAT the traffic, if a user with address 10.0.1.10 connects over SSH to the host with address 10.200.3.1?

- A. 10.200.1.10
- B. 10.0.1.254
- C. 10.200.1.1
- D. 10.200.3.1

Correct Answer: C

Traffic is coming from LAN to WAN, matches policy Full_Access which has NAT enable, so traffic uses source IP address of outgoing interface. Simple SNAT.

QUESTION 5

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

- A. System time
- B. FortiGuard update servers
- C. Operating mode

D. NGFW mode

Correct Answer: CD

C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.

D:

"Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

[NSE4_FGT-7.2 PDF Dumps](#) [NSE4_FGT-7.2 Study Guide](#) [NSE4_FGT-7.2 Braindumps](#)