



NSE4_FGT-6.4^{Q&As}

Fortinet NSE 4 - FortiOS 6.4

Pass Fortinet NSE4_FGT-6.4 Exam with 100% Guarantee

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

https://www.passapply.com/nse4_fgt-6-4.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 the exhibit.

```
config firewall policy
edit 1
set name "INTERNET"
set uuid b11ac58c-791b-51e7-4600-12f829a689d9
set srcintf "port3"
set dstintf "port1"
set srcaddr "LOCAL_SUBNET"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set inspection-mode proxy
set http-policy-redirect enable
set ssl-ssh-profile "certificate-inspection"
set av-profile "default"
set logtraffic all
set logtraffic-start enable
set ippool enable
set poolname "ProxyPool"
set nat enable
next
end

config firewall proxy-address
edit "EICAR"
set uuid 5a24bdaa-c792-51ea-2c89-a9f79e2bdc96
set type host-regex
set host-regex ".*eicar\\.org"
next
end
```

```
config firewall
edit 1
set uuid 6491d126-c790-51ea-1319-4ed94b543a8e
set proxy transparent-web
set srcintf "port3"
set dstintf "port1"
set srcaddr "all"
set dstaddr "EICAR"
set service "webproxy"
set action accept
set schedule "always"
set logtraffic all
set utm-status enable
set ssl-ssh-profile "certificate-inspection"
set av-profile "default"
next
edit 2
set uuid 6a1c74c6-c794-51ea-e646-4f70ae2bc5f9
set proxy transparent-web
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set service "webproxy"
set action accept
set status disable
set schedule "always"
set logtraffic disable
set ssl-ssh-profile "certificate-inspection"
next
edit 3
set uuid 818fb8b6-c797-51ea-d848-a7c2952ceea9
set proxy transparent-web
set srcintf "port3"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set service "webproxy"
set action accept
set status disable
set schedule "always"
set logtraffic all
set utm-status enable
set ssl-ssh-profile "certificate-inspection"
set av-profile "default"
next
end
```

The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses.

How does FortiGate process the traffic sent to <http://www.fortinet.com>?

- A. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 3.
- B. Traffic will not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.
- C. Traffic will be redirected to the transparent proxy and It will be allowed by proxy policy ID 1.
- D. Traffic will be redirected to the transparent proxy and it will be denied by the proxy implicit deny policy.

Correct Answer: D

QUESTION 2



Refer to the exhibit.

Outgoing Interfaces

Manual
Manually assign outgoing interfaces.

Best Quality
The interface with the best measured performance is selected.

Lowest Cost (SLA)
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

Maximize Bandwidth (SLA)
Traffic is load balanced among interfaces that meet SLA targets.

Interface preference

port1	X
port2	X
port3	X
port4	X

Measured SLA: SLA_1

Quality criteria: Latency

Status:

```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check.

Which interface will be selected as an outgoing interface?

- A. port2
- B. port4
- C. port3
- D. port1

Correct Answer: D

QUESTION 3

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

- A. Heuristics scan



- B. Trojan scan
- C. Antivirus scan
- D. Ransomware scan

Correct Answer: A

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/567568/enabling-scanning>

QUESTION 4

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

Correct Answer: CD

QUESTION 5

When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

- A. remote user's public IP address
- B. The public IP address of the FortiGate device.
- C. The remote user's virtual IP address.
- D. The internal IP address of the FortiGate device.

Correct Answer: D

Source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address

[NSE4_FGT-6.4 PDF Dumps](#) [NSE4_FGT-6.4 VCE Dumps](#) [NSE4_FGT-6.4 Study Guide](#)