

# Fortinet

NSE4\_FGT-7.0  
Fortinet NSE 4 - FortiOS 7.0

For More Information – Visit link below:

<https://www.examsempire.com/>

## Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

---

# Latest Version: 8.1

## Question: 1

Refer to Exhibit.

<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a>			
	Interfaces	Gateway	Cost
	virtual-wan-link		
•	port1	10.200.1.254	15
•	port2	10.200.2.254	5
•	port3	10.200.3.254	5
•	port4	10.200.4.254	1

Name: SLA\_1

Detection Mode:  Active  Passive  Prefer Passive

Protocol:  Ping  HTTP  DNS

Servers: 4.2.2.2  4.2.2.1

Participants: All SD-WAN Members 

- port1
- port2
- port3
- port4

Enable probe packets:

SLA Target:

Latency threshold:  50 ms

Jitter threshold:  5 ms

Packet Loss threshold:  0 %

Outgoing Interfaces

Select a strategy for how outgoing interfaces will be chosen.

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
- port2
- port3

```
NGFW-1 # diagnose sys sdwan health-check
Health Check(SLA_1):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x1
Seq(2 port2): state(alive), packet-loss(0.000%) latency(34.349), jitter(3.887) sla_map=0x1
Seq(3 port3): state(alive), packet-loss(0.100%) latency(31.476), jitter(3.254) sla_map=0x1
Seq(4 port4): state(alive), packet-loss(2.130%) latency(46.229), jitter(4.287) sla_map=0x1
```

Refer to Exhibit. The exhibit shows the configuration for the SD-WAN member, Performance SLA, and SD-WAN Rule, 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. port3
- C. port4
- D. port1

**Answer: A**

Port 2 because of its lowest cost against Port1

## Question: 2

Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

- A. FortiGate uses the AD server as the collector agent.
- B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- C. FortiGate does not support workstation check.
- D. FortiGate directs the collector agent to use a remote LDAP server.

**Answer: B D**

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

## Question: 3

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: B C**

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".

## Question: 4

### Exhibit A

The screenshot displays the 'Edit Policy' configuration page in FortiGate. The 'Inspection Mode' is set to 'Flow-based'. Under 'Firewall / Network Options', 'NAT' is enabled, and 'IP Pool Configuration' is set to 'Use Outgoing Interface Address'. 'Preserve Source Port' is disabled. 'Protocol Options' is set to 'PRX default'. Under 'Security Profiles', 'AntiVirus' is enabled and set to 'AV default', while 'Web Filter', 'DNS Filter', 'Application Control', and 'IPS' are disabled. 'SSL Inspection' is enabled and set to 'SSL deep-inspection', and 'Decrypted Traffic Mirror' is disabled.

Section	Option	Value
Inspection Mode	Flow-based	Selected
	Proxy-based	Not Selected
Firewall / Network Options	NAT	Enabled
	IP Pool Configuration	Use Outgoing Interface Address
	Use Dynamic IP Pool	Not Selected
	Preserve Source Port	Disabled
Protocol Options	PRX default	Selected
Security Profiles	AntiVirus	Enabled, AV default
	Web Filter	Disabled
	DNS Filter	Disabled
	Application Control	Disabled
	IPS	Disabled
	SSL Inspection	Enabled, SSL deep-inspection
	Decrypted Traffic Mirror	Disabled

## Exhibit B

**Edit AntiVirus Profile**

Name

Comments  29/255

Detect Viruses  Block  Monitor

Feature set  Flow-based  Proxy-based

**Inspected Protocols**

HTTP

SMTP

POP3

IMAP

FTP

CIFS

**APT Protection Options**

Treat Windows Executables in Email Attachments as Viruses

Include Mobile Malware Protection

**Virus Outbreak Prevention** ⓘ

Use FortiGuard Outbreak Prevention Database

Use External Malware Block List ⓘ ⚠

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B). Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The firewall policy performs the full content inspection on the file.
- B. The flow-based inspection is used, which resets the last packet to the user.
- C. The volume of traffic being inspected is too high for this model of FortiGate.
- D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

---

**Answer: B**

Explanation:

- "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately
- When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.

In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

### Question: 5

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: B C E**

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-andreporting-overview>

## Thank You for Trying Our Product

Discount Coupon Code is: **20OFF2022**

**Email:** [support@examsempire.com](mailto:support@examsempire.com)

**Check our Customer Testimonials and ratings  
available on every product page.**

**Visit our website.**

**<https://examsempire.com/>**