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.pass4itsure.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

QUESTION 1

Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

A. To allow for out-of-order packets that could arrive after the FIN/ACK packets

B. To finish any inspection operations

C. To remove the NAT operation

D. To generate logs

Correct Answer: A

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an entry in the firewall session table.

QUESTION 2

Which two statements describe how the RPF check is used? (Choose two.)

A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

B. The RPF check is run on the first sent and reply packet of any new session.

C. The RPF check is run on the first sent packet of any new session.

D. The RPF check is run on the first reply packet of any new session.

Correct Answer: AC

FortiGate Infrastructure 7.2 Study Guide (p.41): "The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table." "FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn\\'t perform any additional RPF checks on that session."

A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks. This is true because the RPF check verifies that the source IP address of an incoming packet matches the reverse route for that address, meaning that the packet came from a legitimate source and not from an attacker who is trying to impersonate another host. This prevents IP spoofing attacks, where an attacker sends packets with a forged source IP address to bypass security policies or launch denial-of-service attacks1 C. The RPF check is run on the first sent packet of any new session. This is true because the RPF check is performed only once per session, on the first packet sent by either the client or the server, depending on the direction of the session initiation. This reduces the processing overhead and improves performance2

QUESTION 3

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning

B. Exempt

C. Allow

D. Learn

Correct Answer: AC

QUESTION 4

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.

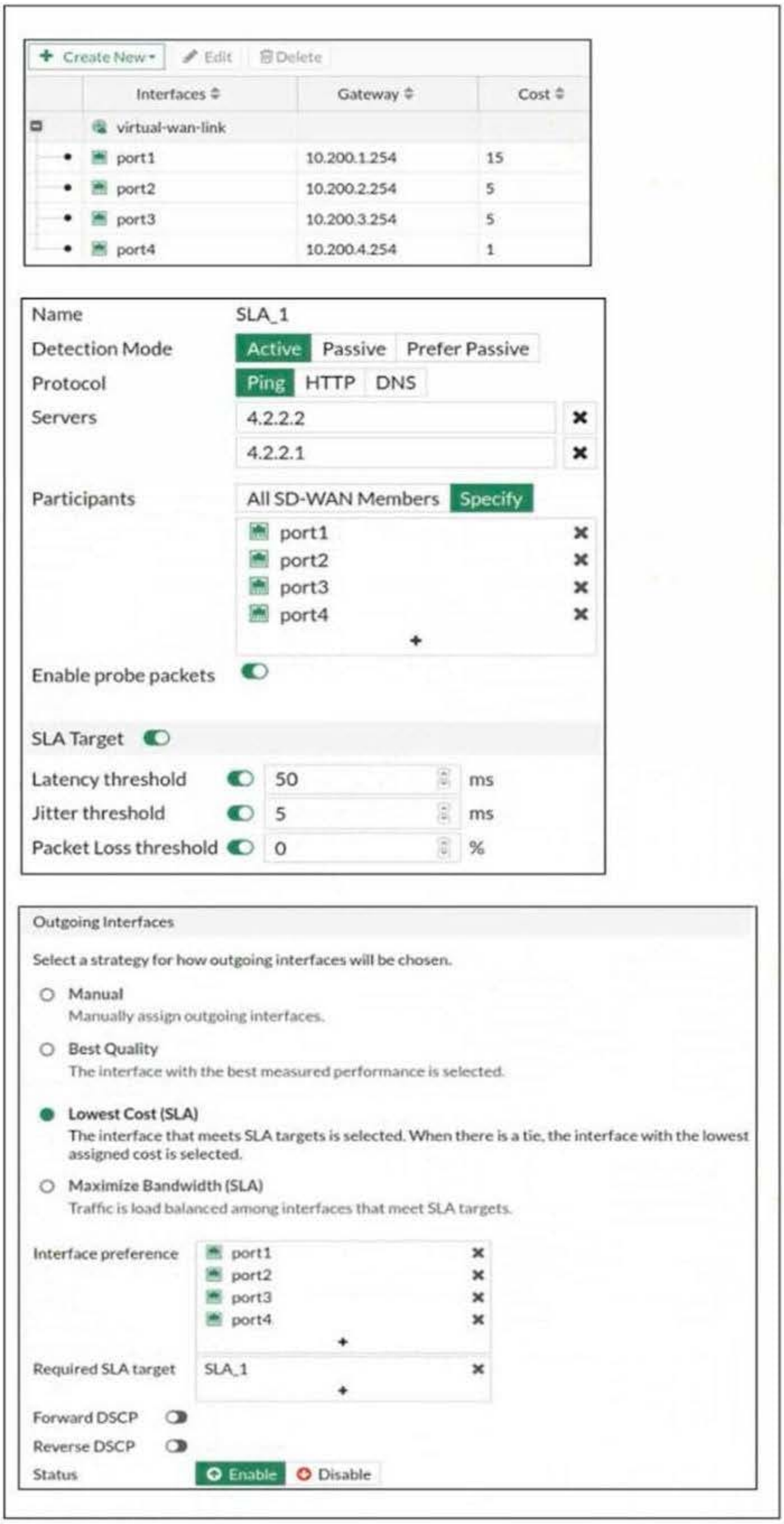
D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/190873/video-filtering

QUESTION 5

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.



	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 [✓ Specify] 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.

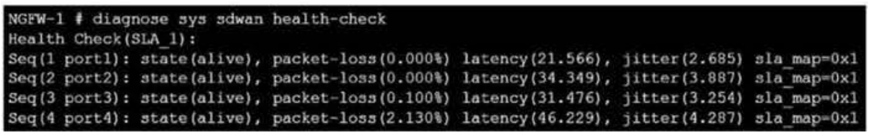
○ Manual
Manually assign outgoing interfaces.

○ 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 ✖ port4 ✖ +
Required SLA target	SLA_1 ✖ +
Forward DSCP	○
Reverse DSCP	○
Status	[✓ Enable] Disable



```
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
```

Which interface will be selected as an outgoing interface?

A. port2

B. port3

C. port4

D. port1

Correct Answer: A

To determine the best path for traffic in Fortinet\\'s SD-WAN implementation, a "lowest cost" algorithm is used that considers the cost metric associated with each available WAN link. In this case, Port 4 and 3 are eliminated due to packet loss,

leaving Port 1 and Port 2 as the available paths.

The next stage of elimination is based on the highest cost. Port 1 has a high cost of 15, which makes it less desirable than Port 2. Therefore, Port 1 is eliminated, and Port 2 is selected as the winner.