FortiDDoS.VCEplus.premium.exam.15q

Number: FortiDDoS
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

FortiDDoS

FortiDDoS 4.0 Specialist

Version 1.0

Exam A

QUESTION 1
Which is true regarding packets that match a do-not-track policy with the action Track and Allow?

A. Packets are never dropped.
B. Source IP addresses are added to the legitimate IP (LIP) table.
C. Packets are not included in the statistics for threshold estimation.
D. Packets are assigned to SPP 0.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://help.fortinet.com/fddos/4-3-0/FortiDDoS/Configuring_a_Do_Not_Track_policy.htm

QUESTION 2
Regarding the switching SPP feature, what is used to determine when FortiDDoS switches the traffic to an alternate SPP?

A. Traffic volume
B. Destination IP addresses
C. Mitigated attacks
D. Blocked packets

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://help.fortinet.com/fddos/4-3-0/FortiDDoS/Configuring_SPP_policy_settings.htm

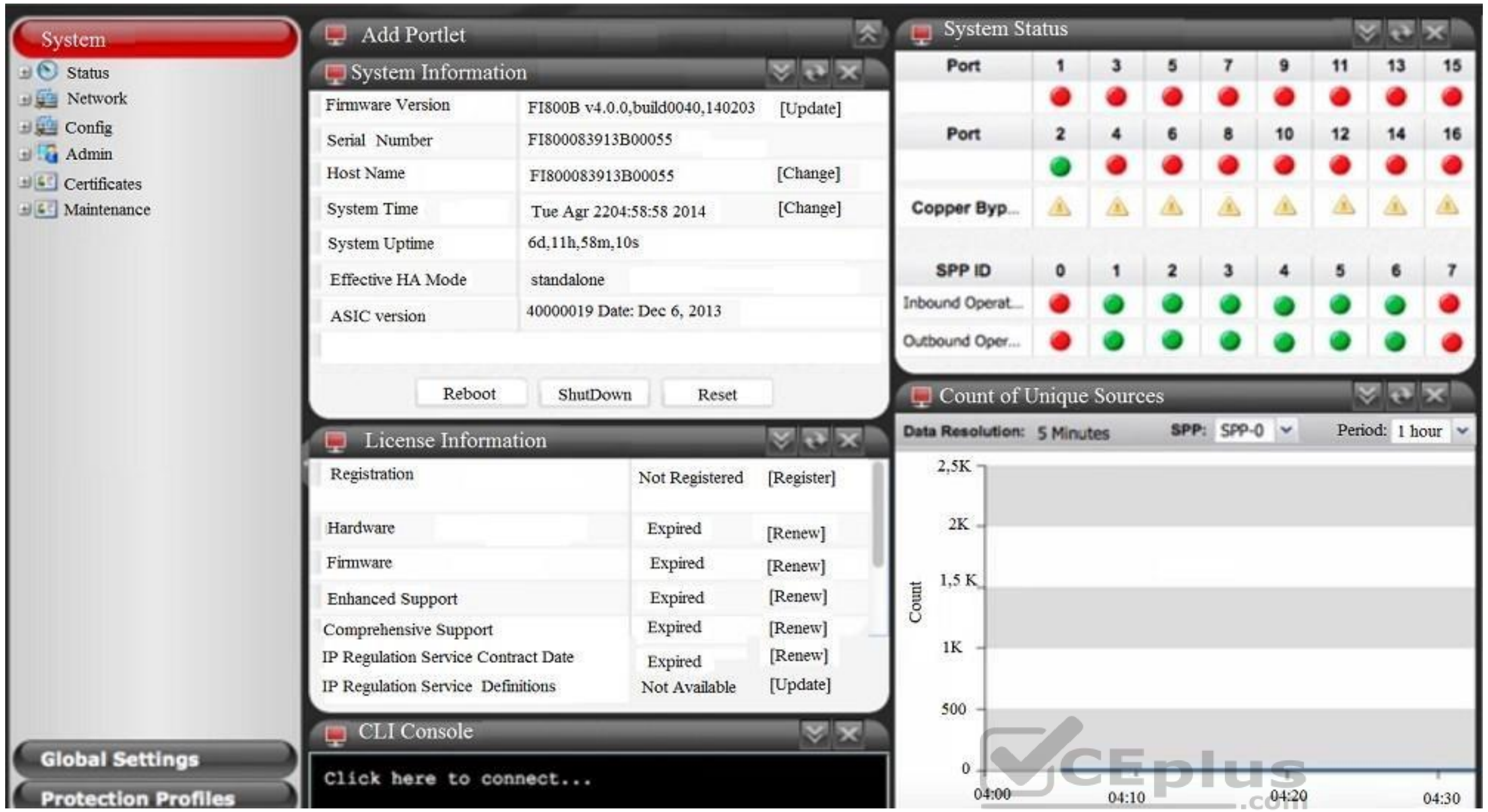
QUESTION 3
A FortiDDoS device is connected between a protected server and an Internet router. For the aggressive aging feature, the administrator must manually add the router internal interface MAC address to the FortiDDoS configuration. Why does the FortiDDoS need this information?

A. To send RST packets to the protected server spoofing the router internal interface MAC address.
B. To allow incoming traffic only from that specific MAC address.
C. To determine which traffic direction is incoming and which traffic direction is outgoing.
D. To allow outgoing traffic only to that specific MAC address.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://s3.amazonaws.com/fortinetweb/docs.fortinet.com/v2/attachments/44f876f1-2436-11e9-b20a-f8bc1258b856/fortiddos-5-0-0-handbook.pdf page 80

QUESTION 4
As the exhibit shows, a FortiDDoS port2 is connected to the protected server. Its port1 is connected to the Internet. The FortiDDoS has 8 interfaces for user traffic. The exhibit also shows a screenshot of the unit dashboard.



System Information

Firmware Version	FI800B v4.0.0,build0040,140203	[Update]
Serial Number	FI800083913B00055	
Host Name	FI800083913B00055	[Change]
System Time	Tue Agr 2204:58:58 2014	[Change]
System Uptime	6d,11h,58m,10s	
Effective HA Mode	standalone	
ASIC version	40000019 Date: Dec 6, 2013	

License Information

Registration	Not Registered	[Register]
Hardware	Expired	[Renew]
Firmware	Expired	[Renew]
Enhanced Support	Expired	[Renew]
Comprehensive Support	Expired	[Renew]
IP Regulation Service Contract Date	Expired	[Renew]
IP Regulation Service Definitions	Not Available	[Update]

CLI Console

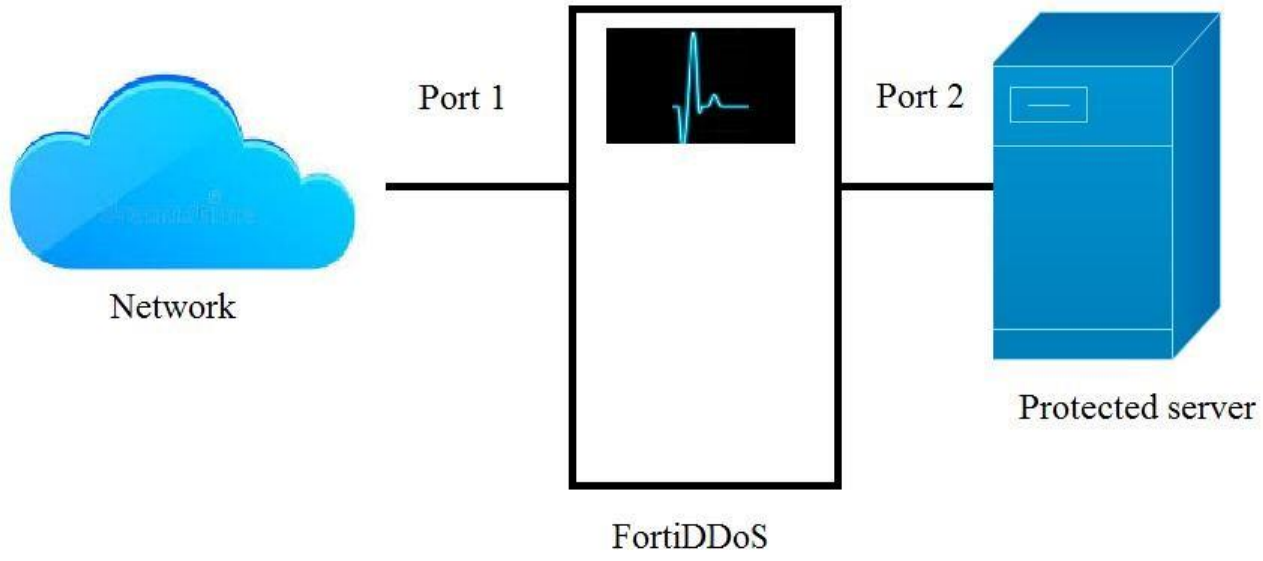
```
Click here to connect...
```

System Status

Port	1	3	5	7	9	11	13	15
	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Port	**2**	**4**	**6**	**8**	**10**	**12**	**14**	**16**
	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Copper Byp...	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
SPP ID	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Inbound Operat...	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🔴
Outbound Oper...	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🔴

Count of Unique Sources

Data Resolution: 5 Minutes SPP: SPP-0 Period: 1 hour



The administrator noticed that the statistics are showing all the traffic coming from the Internet to the protected server as outbound, instead of inbound. Based on the exhibit, what is the cause of this mislabeling?

A. The protected server is connected to a wrong FortiDDoS interface. It must be connected to an interface from port 5 to port 8.
B. SPP 0 is operating in detection mode.
C. The SPP 0 link is down.
D. FortiDDoS interfaces are wrongly connected. The interface port1 must be connected to the protected server and port2 must be connected to the Internet.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

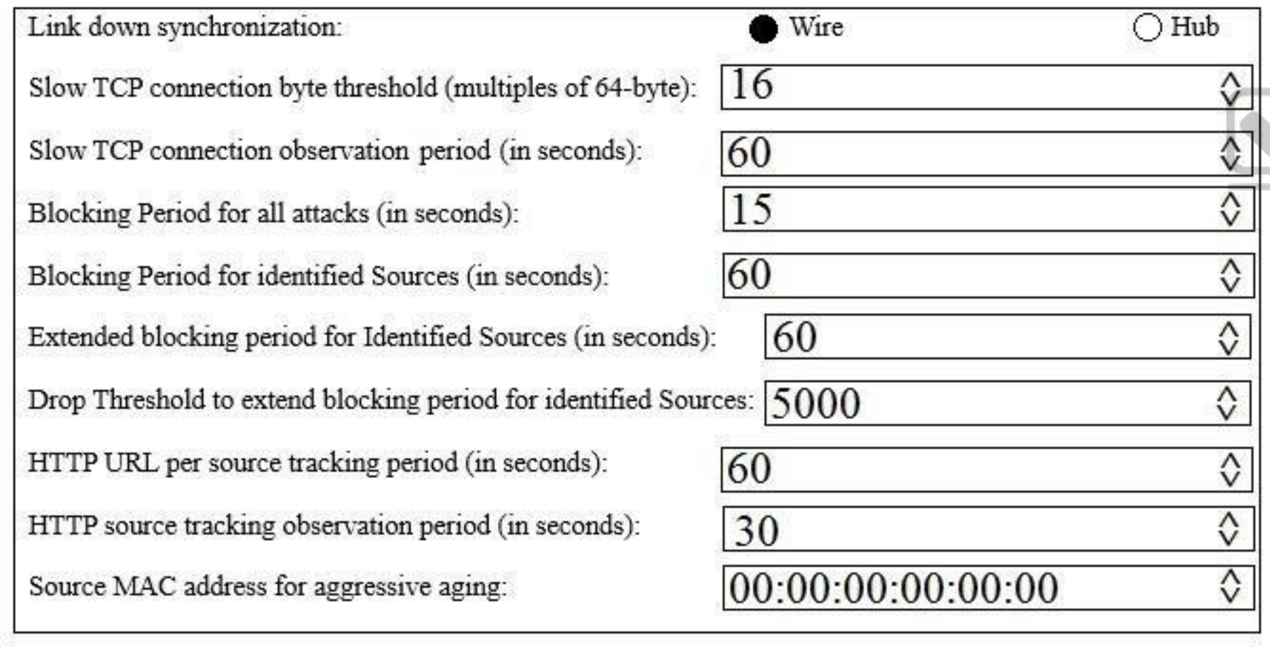
QUESTION 5
A FortiDDoS administrator wants the configured minimum threshold to act as a hard, fixed threshold. So, FortiDDoS will start dropping packets and mitigating the traffic as soon as the traffic volume goes above the configured minimum threshold, regardless of the values of the other thresholds. What configuration change can be done to achieve this requirement?

A. Setting the SPP to detection mode.
B. Changing the adaptive mode to fixed.
C. Setting the adaptive limit percentage to 100%.
D. Disabling the adaptive limit threshold.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://s3.amazonaws.com/fortinetweb/docs.fortinet.com/v2/attachments/44f876f1-2436-11e9-b20a-f8bc1258b856/fortiddos-5-0-0-handbook.pdf page 63

QUESTION 6
The exhibit shows the configuration for the blocking periods.



Link down synchronization: ● Wire ○ Hub
Slow TCP connection byte threshold (multiples of 64-byte): 16
Slow TCP connection observation period (in seconds): 60
Blocking Period for all attacks (in seconds): 15
Blocking Period for identified Sources (in seconds): 60
Extended blocking period for Identified Sources (in seconds): 60
Drop Threshold to extend blocking period for identified Sources: 5000
HTTP URL per source tracking period (in seconds): 60
HTTP source tracking observation period (in seconds): 30
Source MAC address for aggressive aging: 00:00:00:00:00:00

FortiDDoS has detected an incoming fragmented flood attack in SPP 0
According with the exhibit, which action does the unit take with the SPP-0 traffic as soon as the attack is detected?

A. Incoming fragmented packets from all sources are blocked for at least 60 seconds.
B. Incoming fragmented packets from all identified malicious sources are blocked for at least 120 seconds.
C. Incoming fragmented packets from all sources are blocked for at least 15 seconds.
D. All incoming packets from all sources are blocked for at least 15 seconds.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://s3.amazonaws.com/fortinetweb/docs.fortinet.com/v2/attachments/44f876f1-2436-11e9-b20a-f8bc1258b856/fortiddos-5-0-0-handbook.pdf page 264

QUESTION 7 A FortiDDoS device must be deployed as soon as possible in a customer network that is currently under a DDoS attack. Which values are recommended to use for the configured minimum thresholds?

A. The factory default values.
B. The factory default values increased by a percentage that depends on the customer traffic volume.
C. The easy setup values.
D. The system recommended values after a one-hour learning period.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://s3.amazonaws.com/fortinetweb/docs.fortinet.com/v2/attachments/44f876f1-2436-11e9-b20a-f8bc1258b856/fortiddos-5-0-0-handbook.pdf page 126

QUESTION 8 Which of the following DoS attacks are categorized as bulk volumetric attacks?
(Choose two.)

A. Slowloris
B. HTTP slow read
C. SYN flood
D. ICMP flood

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 What is the maximum number of service protection profiles (SPPs) supported in a FortiDDoS device?

A. 2
B. 4
C. 8
D. 16

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://s3.amazonaws.com/fortinetweb/docs.fortinet.com/v2/attachments/44f876f1-2436-11e9-b20a-f8bc1258b856/fortiddos-5-0-0-handbook.pdf page 17

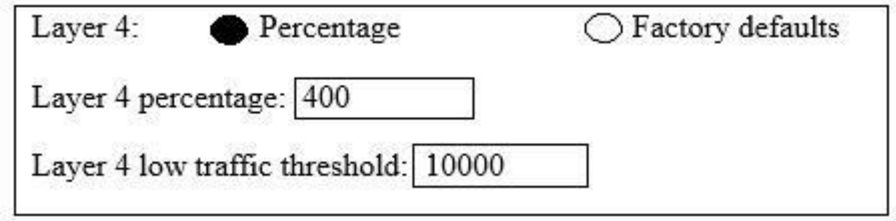
QUESTION 10
A FortiDDoS device is configured to mitigate SYN flood attacks using the SYN cookie mode. What action does it take when it is mitigating an SYN flood attack and a SYN packet from a new source IP address arrives?

A. It replies with a SYN/ACK packet containing a cookie value in the TCP sequence field.
B. It replies with a SYN/ACK packets. One containing the right acknowledge value, the other one with a wrong acknowledge value.
C. It replies with a RST packet if the SYN packet does not contain the right cookie in the sequence field.
D. It replies with a SYN/ACK packet containing a cookie value in the TCP acknowledge field.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://s3.amazonaws.com/fortinetweb/docs.fortinet.com/v2/attachments/44f876f1-2436-11e9-b20a-f8bc1258b856/fortiddos-5-0-0-handbook.pdf page 78

QUESTION 11
The exhibit shows the partial configuration settings to generate the system recommended values for the configured minimum thresholds.



Layer 4: ● Percentage ○ Factory defaults

Layer 4 percentage: 400

Layer 4 low traffic threshold: 10000

During the learning period, the maximum packet rate for UDP traffic to port 53 was 2,000 packets per second. According with the exhibit, what will be the system recommended value for the configured minimum threshold for UDP traffic to port 53?

A. 8,000 packets per second
B. 2,000 packets per second
C. 400 packets per second
D. 10,000 packets per second

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://s3.amazonaws.com/fortinetweb/docs.fortinet.com/v2/attachments/44f876f1-2436-11e9-b20a-f8bc1258b856/fortiddos-5-0-0-handbook.pdf page 361

QUESTION 12 Which of the following events can make FortiDDoS drop packets?
(Choose two.)

A. SPPs are working in detection mode.
B. Packets match an access list with action deny.
C. One direction of the traffic is crossing the FortiDDoS, but the other direction is not (asymmetric routing).
D. A violation of the TCP protocol in a TCP session.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 What events are recorded in the system event logs?
(Choose two.)

A. traffic mitigation events
B. blocking events
C. system restarts
D. configuration changes

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14 The setting **Link Down Synchronization** has been configured as **Wire.** What happens if the port link status goes down?

A. FortiDDoS disables its interface port2.
B. Traffic will be automatically rerouted through interface port2.
C. SPP 1 goes to detection mode.
D. Traffic will be automatically rerouted through interface port3.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://s3.amazonaws.com/fortinetweb/docs.fortinet.com/v2/attachments/44f876f1-2436-11e9-b20a-f8bc1258b856/fortiddos-5-0-0-handbook.pdf page 40

QUESTION 15 What information is synchronized between two FortiDDoS devices that are part of the same HA cluster? (Choose two.)

A. Digital certificates
B. Configured minimum threshold
C. Reports
D. Estimated thresholds

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference: