FCNSP.V5 Q&As

Fortinet Certified Network Security Professional (FCNSP.v5)

Pass Fortinet FCNSP.V5 Exam with 100% Guarantee

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

https://www.passapply.com/fcnsp-v5.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An administrator is examining the attack logs and notices the following entry:

device_id=FG100A3907508962 log_id=18432 subtype=anomaly type=ips timestamp=1270017358 pri=alert itime=1270017893 severity=critical src=192.168.1.52 dst=64.64.64.64 src_int=internal serial=0 status=clear_session proto=6 service=http vd=root count=1 src_port=35094 dst_port=80 attack_id=100663402 sensor=protect-servers ref=http://www.fortinet.com/ids/VID100663402 msg="anomaly: tcp_src_session, 2 > threshold 1" policyid=0 carrier_ep=N/A profile=N/A dst_int=N/A user=N/A group=N/A

Based solely upon this log message, which of the following statements is correct?

A. This attack was blocked by the HTTP protocol decoder.

B. This attack was caught by the DoS sensor "protect-servers".

C. This attack was launched against the FortiGate unit itself rather than a host behind the FortiGate unit.

D. The number of concurrent connections to destination IP address 64.64.64.64 has exceeded the configured threshold.

Correct Answer: B

QUESTION 2

Which of the following describes the difference between the ban and quarantine actions?

A. A ban action prevents future transactions using the same protocol which triggered the ban. A qarantine action blocks all future transactions, regardless of the protocol.

B. A ban action blocks the transaction. A quarantine action archives the data.

C. A ban action has a finite duration. A quarantine action must be removed by an administrator.

D. A ban action is used for known users. A quarantine action is used for unknown users.

Correct Answer: A

QUESTION 3

Select the answer that describes what the CLI command diag debug authd fsso list is used for.

A. Monitors communications between the FSSO Collector Agent and FortiGate unit.

B. Displays which users are currently logged on using FSSO.

C. Displays a listing of all connected FSSO Collector Agents.

D. Lists all DC Agents installed on all Domain Controllers.

Correct Answer: B

QUESTION 4

An administrator wishes to generate a report showing Top Traffic by service type. They notice that web traffic overwhelms the pie chart and want to exclude the web traffic from the report.

Which of the following statements best describes how to do this?

A. In the Service field of the Data Filter, type 80/tcp and select the NOT checkbox.

B. Add the following entry to the Generic Field section of the Data Filter: service="!web".

C. When editing the chart, uncheck wlog to indicate that Web Filtering data is being excluded when generating the chart.

D. When editing the chart, enter \\'http\\' in the Exclude Service field.

Correct Answer: A

QUESTION 5

An organization wishes to protect its SIP Server from call flooding attacks. Which of the following configuration changes can be performed on the FortiGate unit to fulfill this requirement?

A. Apply an application control list which contains a rule for SIP and has the "Limit INVITE Request" option configured.

B. Enable Traffic Shaping for the appropriate SIP firewall policy.

C. Reduce the session time-to-live value for the SIP protocol by running the configure system session-ttl CLI command.

D. Run the set udp-idle-timer CLI command and set a lower time value.

Correct Answer: A