NSE4 Q&As

Fortinet Network Security Expert 4 Written Exam (400)

Pass Fortinet NSE4 Exam with 100% Guarantee

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

https://www.geekcert.com/nse4.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

If you enable the option "Generate Logs when Session Starts", what effect does this have on the number of traffic log messages generated for each session?

A. No traffic log message is generated.

B. One traffic log message is generated.

C. Two traffic log messages are generated.

D. A log message is only generated if there is a security event.

Correct Answer: C

QUESTION 2

Which type of conserve mode writes a log message immediately, rather than when the device exits conserve mode?

A. Kernel

B. Proxy

C. System

D. Device

Correct Answer: B

QUESTION 3

What determines whether a log message is generated or not?

A. Firewall policy setting

B. Log Settings in the GUI

C. \\'config log\\' command in the CLI

D. Syslog

E. Webtrends

Correct Answer: A

QUESTION 4

Which of the following email spam filtering features is NOT supported on a FortiGate unit?

A. Multipurpose Internet Mail Extensions (MIME) Header Check

B. HELO DNS Lookup

C. Greylisting

D. Banned Word

Correct Answer: C

QUESTION 5

You are creating a custom signature. Which has incorrect syntax?

A. F-SBID(--attack_id 1842,--name "Ping.Death";--protocol icmp; --data_size>32000;)

B. F-SBID(--name "Block.SMTP.VRFY.CMD";--pattern "vrfy";-- service SMTP; --no_case;-- context header;)

C. F-SBID(--name "Ping.Death";--protocol icmp;--data_size>32000;)

D. F-SBID(--name "Block".HTTP.POST"; --protocol tcp;-- service HTTP;-- flow from_client; --pattern "POST"; -- context uri;--within 5,context;)

Correct Answer: A

NSE4 VCE Dumps NSE4 Practice Test NSE4 Study Guide