Fortinet

NSE6_DDS_AD-7.2

Fortinet NSE 6 - FortiDDoS 7.2 Administrator

Latest Version: 6.0

Question: 1

During a severe attack an operator notices that attack log entries, which had been appearing at five-minute intervals, begin arriving every minute.
What has happened?

A. The local log filled, so the appliance began flushing partial records more frequently
B. The event is interrupt-driven and its drop count exceeded the system thresholds
C. The appliance switched from periodic to interrupt-driven reporting when the policy entered Prevention Mode
D. An administrator changed the logging interval while the attack was under way

Answer: B

Question: 2

What does Cloud Signaling do when an attack exceeds the configured rate for a service protection policy?

A. It signals a Fortinet cloud DDoS partner that a large attack is under way and sends attack log detail
B. It moves the affected policy into Prevention Mode automatically for the duration of the attack
C. It redirects the traffic through the appliance's second interface pair for scrubbing
D. It raises the local thresholds temporarily so the appliance can absorb the additional volume

Answer: A

Question: 3

An operator is considering the ACK Cookie method rather than SYN Cookie for a protected zone.
What condition makes ACK Cookie a reasonable choice?

A. Sufficient reverse path bandwidth to carry the additional packets it generates
B. A deployment configured for asymmetric operation where the return path is not visible
C. A protected service that uses long-lived connections rather than many short ones
D. A policy that has completed its learning period and moved to Prevention Mode

Answer: A

Question: 4

FortiDDoS models traffic using a historical baseline that weights recent data more heavily, a trend or slope component, and a seasonality component.
What does the seasonality component contribute that the other two cannot?

A. Recognition that traffic grows steadily over months as users are added
B. Recognition that the most recent observations describe current conditions better than older ones do
C. Recognition that an attack in progress should be excluded from the statistics being gathered
D. Recognition that traffic repeats a pattern by time of day and day of week

Answer: D

Question: 5

Which deployment arrangement places FortiDDoS outside the traffic path, so that it observes a copy of the traffic and cannot drop any of it?

A. LACP port channel
B. Tap Mode
C. Built-in fail-open bypass
D. External bypass

Answer: B

Question: 6

Traffic to a protected server is being dropped even though the Layer 3 rate for that policy is well under its threshold.
What does this indicate about how the limits are applied?

A. The Layer 3 threshold is advisory and only the Layer 7 limits are actually enforced on traffic
B. The lowest configured threshold across all layers is the only one that ever takes effect
C. The layers are evaluated in order, stopping at the first one satisfied
D. A packet must satisfy the applicable threshold at every layer

Answer: D

Question: 7

How is configuration kept consistent between the two nodes of a FortiDDoS HA cluster?

A. Each node writes its own changes independently and the pair reconciles by keeping whichever version carries the newer timestamp
B. The primary pushes its configuration to the secondary at initialization and periodically afterwards
C. Both nodes pull their configuration, and their thresholds, from a management station on a schedule
D. An administrator exports the configuration from one node and imports it on the other after every change is made

Answer: B

Question: 8

Why is service degradation treated as a DDoS outcome in its own right, rather than only as a step on the way to an outage?

A. Degradation indicates an application-layer attack
B. Only during degradation can mitigation still be applied
C. Only degradation leaves traffic for the appliance to measure
D. A slow service is already costing the business

Answer: D

Question: 9

By default, how far above the configured minimum threshold may the adaptive limit allow a value to rise?

A. There is no ceiling on the estimate
B. To 100 percent of it, meaning no upward movement is permitted at all
C. To 150 percent of it
D. To 500 percent of it, giving substantial room for seasonal growth over time

Answer: C

Question: 10

In a reflected amplification attack, why does the attacker place the victim's address in the source field of the queries it sends?

A. So the responses look like replies to a session already open
B. So the victim's firewall accepts the queries as internally originated traffic

C. So the third-party servers cannot record who issued the queries
D. So the third-party servers send their larger responses to the victim

Answer: D

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer