DUMPSBOSS.

McAfee Certified Product Specialist – NSP

McAfee MA0-101

Version Demo

Total Demo Questions: 11

Total Premium Questions: 114

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Network Security Platform Architecture	34
Topic 2, Network Security Platform Installation	4
Topic 3, Network Security Platform Configuration	42
Topic 4, Network Security Platform Administration	23
Topic 5, Network Security Platform Troubleshooting	10
Topic 6, Mix Questions	1
Total	114

QUESTION NO: 1

Which of the following should be completed before upgrading Sensor software? (Choose three)

A. Verify that the image supports the Sensor model

B. Back up the current Sensor configuration

C. Schedule a maintenance window

D. Delete the assigned policy

E. Disable all attack signatures permanently

ANSWER: A B C

Explanation:

Before a Sensor software upgrade, administrators should **verify image compatibility** with the Sensor model and current deployment, **back up the existing configuration**, and **schedule an appropriate maintenance window**. Compatibility verification helps prevent an unsupported image from being assigned to the appliance. A current backup supports recovery if an unexpected issue occurs, and a maintenance window accounts for the reboot and possible interruption to inline inspection.

Deleting the existing policy is not required and can create unnecessary configuration loss. Disabling all signatures is also not a prerequisite for a software upgrade. Current software images and release-specific upgrade procedures are available through Trellix Support Downloads and the Trellix Documentation Portal.

QUESTION NO: 2

Which command is used to manually download signature tiles from the tftpserver when connectivity to the Manager is not available?

A. Loadimage WORD

B. Loadconfig WORD

C. Loadconfiguration WORD

D. Loadsigset WORD

ANSWER: D

Explanation:

`Loadsigset WORD` is the Sensor command intended for manually retrieving and loading a signature set from a TFTP server. In Network Security Platform terminology, signature updates are distributed as signature-set content, including the signature tiles needed by the Sensor detection engine. Normally, Manager coordinates Sensor updates, but a TFTP-based manual load provides an administrative recovery path when the Sensor cannot communicate with Manager. The value represented by `WORD` is supplied with the TFTP location and/or signature-set file information required by the Sensor CLI for the transfer. After the set is obtained and validated, the Sensor can use the newly loaded signatures without relying on a current Manager connection for the download operation. This procedure is specifically for signature content, rather than software-image installation or configuration retrieval, and should be performed using signature files that match the Sensor model and supported software release. Trellix maintains the Network Security Platform documentation collection at Network Security Platform Product Guide; product documentation and downloads are also available from the Trellix Support Downloads page.

QUESTION NO: 3

What is the primary purpose of a packet log associated with an attack alert?

A. Captured packet data for investigation of the alert

B. A backup of the Sensor configuration

C. A record of Manager user logins

D. A replacement for signature updates

ANSWER: A

Explanation:

A packet log provides **captured packet data for investigation of the alert**. It allows an administrator to examine the traffic that caused or was associated with an attack event, including packet headers, protocol details, sequence information, and available payload data.

Packet logs provide more forensic context than an alert summary alone. They can help an analyst validate the event, determine the direction and scope of the activity, and identify whether the observed traffic represents a true attack or requires additional policy tuning. Packet logs do not replace Sensor configuration backups or Manager audit logs. See the Wireshark documentation and the Trellix Product Documentation portal for packet-analysis and Network Security Platform guidance.

QUESTION NO: 4

Which sensor action allows the detection and dropping of attacks in real-time?

A. Host Quarantine action

B. ICMP Host unreachable

C. TCP reset

D. Drop further packets

ANSWER: D

Explanation:

Drop further packets is the sensor response action that provides real-time inline prevention for a detected attack. When a Network Security Platform sensor is deployed inline and a signature matches traffic, the sensor can continue inspecting the flow while discarding subsequent packets associated with that attack. This lets the sensor actively stop malicious traffic as it traverses the network rather than merely recording the event for later review. The response is particularly useful when the sensor has identified an attack pattern within an active session and must prevent the remaining payload, commands, or exploit traffic from reaching its destination.

Real-time dropping depends on the sensor being positioned and configured for inline operation, because the sensor must be in the traffic path to enforce a packet-discard decision. In this mode, Network Security Platform combines signature-based detection with prevention actions, allowing policy authors to assign an appropriate response to each attack definition. The event is also available to management and monitoring components, providing visibility into the prevented intrusion while enforcement occurs immediately on the sensor. See the Trellix Network Security product information and the Trellix Product Documentation portal for Network Security Platform documentation.

QUESTION NO: 5

Which of the following are the methods used by NSP to recognize and react to Denial-of-Service (DoS) attacks? (Choose three)

A. Blocking

B. Shutting down the sensor

C. Thresholds

D. Self-learning

E. Logging

F. DDoS attack tool with exploit signatures

ANSWER: C D F

Explanation:

Network Security Platform (NSP) identifies DoS and DDoS activity through a combination of rate-based detection, adaptive baselining, and signature-based inspection. **Thresholds** provide rate-based detection: administrators can define limits for events such as connection attempts, packets, or traffic volumes over a period. When observed traffic exceeds the configured level, NSP can generate an alert and apply the configured response. **Self-learning** enables the sensor to establish a baseline for normal traffic behavior and recognize anomalous increases that are characteristic of flooding or resource-exhaustion attacks. This is particularly useful where a fixed threshold would not fit changing traffic patterns. **DDoS attack tool with exploit signatures** represents NSP's signature-based coverage for known attack tools and their traffic patterns. Signature inspection allows the sensor to recognize documented malicious techniques rather than relying solely on volume measurements. Together, these mechanisms cover anomalous traffic rates, deviations from learned normal behavior, and known DDoS attack patterns, allowing policies to alert and, where configured, take enforcement action. Trellix maintains Network Security Platform as an intrusion-prevention product; see the Network Security Platform product page and the Trellix support downloads portal for product documentation and releases.

QUESTION NO: 6

Which of the following modes can be used to implement DoS detection? (Choose two)

A. Learning Mode

B. Threshold Mode

C. Configuration Mode

D. Adaptive Mode

E. Transition Mode

ANSWER: A B

Explanation:

DoS detection on McAfee Network Security Platform sensors can be implemented using **Learning Mode** and **Threshold Mode**. Learning Mode establishes a baseline of normal traffic behavior for the monitored network. The sensor observes traffic characteristics such as connection rates, packet rates, bandwidth use, and host activity, then uses the learned baseline to help identify abnormal traffic volumes that may indicate a denial-of-service condition. This approach is useful where normal traffic patterns vary and a static limit would be difficult to define accurately.

Threshold Mode implements DoS detection by applying administrator-defined limits to relevant traffic or resource measurements. When observed activity exceeds the configured threshold, the sensor can generate an alert and, where configured, enforce a response. This provides predictable control when the organization knows the acceptable capacity or transaction rate of a protected service. McAfee Network Security Platform documentation describes DoS protection as policy-based detection using learned behavior or configured thresholds, allowing deployments to select the method appropriate to the network and protected application. See the Trellix Network Security Platform product information and the Network Security Platform solution brief.

QUESTION NO: 7

Which of the following conditions are required for a Sensor to drop attack traffic? (Choose three)

A. The Sensor is deployed in-line

B. The attack response is configured to drop traffic

C. The applicable policy is assigned to the Sensor or interface

D. The Sensor monitoring port is configured as a SPAN destination

E. Packet logging is enabled for all attacks

ANSWER: A B C

Explanation:

A Sensor must be deployed **in-line**, the relevant attack must have an enabled **drop response**, and the applicable **policy must be assigned** to the Sensor or interface handling the traffic. Inline placement gives the Sensor control of the production packet path. The attack response determines whether a matching attack is blocked rather than only reported, and the assigned policy supplies the active inspection configuration.

A SPAN deployment provides a copy of traffic and cannot directly drop the original packets. Packet logging is useful for investigation, but it is not a prerequisite for blocking. See the Trellix Network Security Platform product information and the Trellix Documentation Portal for policy and deployment guidance.

QUESTION NO: 8

Which of the following are benefits of using domains in Network Security Manager? (Choose three)

A. Organizing Sensors by administrative group

B. Delegating administration

C. Inheriting policies from a parent domain

D. Encrypting monitored traffic

E. Replacing Sensor management channels

ANSWER: A B C

Explanation:

Organizing Sensors by administrative group, **delegating administration**, and **inheriting policies from a parent domain** are benefits of the Network Security Manager domain hierarchy. Domains provide a way to organize Sensors and other managed objects according to a logical administrative structure, such as geographic region, business unit, or security operations team.

Domain-based administration also permits appropriate administrative responsibilities to be delegated without granting every administrator access to all managed Sensors. A child domain initially inherits applicable policy assignments from its parent domain, which provides a consistent security baseline while still allowing more specific configuration where authorized. Domains do not encrypt monitored traffic and do not replace the Sensor-to-Manager management connection. See the Trellix Product Documentation portal for Network Security Manager administration information.

QUESTION NO: 9

When the buffer on the alert cache has been filled, what happens to current incoming alerts?

A. Incoming alerts are added to the cache and the oldest alerts are dropped

B. Incoming alerts are not added to the cache and are dropped

C. Incoming alerts are held in queue until cache space is cleared

D. Incoming alerts are added to the database directly

ANSWER: A

Explanation:

Incoming alerts are added to the cache and the oldest alerts are dropped is correct. The Network Security Platform alert cache is a finite, temporary storage area used to retain alert information while it is processed and made available to the Manager and its alert database. It is designed as a rolling buffer rather than as a mechanism that pauses alert generation or guarantees indefinite retention. Once the configured cache capacity has been reached, the platform must make room for the newest alert records. It does so by replacing the oldest cached alerts with current incoming alerts.

This behavior ensures that the system continues accepting and processing the most recent security events, which are generally the most operationally useful during active monitoring and incident response. It also means that cache capacity should be sized appropriately and that alert processing, database connectivity, and Manager health should be monitored so alerts are transferred out of temporary storage promptly. A persistently full alert cache can result in loss of older alert records, so administrators should investigate sustained backlogs and tune retention or processing resources as needed. See the Trellix product documentation portal and Trellix Support for Network Security Platform documentation and configuration guidance.

QUESTION NO: 10

What type of encryption is used for packet log transfers between the Sensor and the Manager?

A. SSL with RC4

B. SSL with MD5

C. SSL with RC4 and MD5

D. DES

ANSWER: C

Explanation:

SSL with RC4 and MD5 is the correct historical Network Security Platform answer for protected packet-log transfers between a Sensor and its Manager. In this SSL configuration, RC4 provides the symmetric encryption used to protect the confidentiality of the transferred packet-log data, while MD5 is used by the SSL protocol suite for message integrity/authentication functions. Therefore, the expected exam wording identifies both components of the SSL protection mechanism rather than naming only the encryption algorithm or only the digest algorithm.

This refers to the legacy protocol implementation and terminology used by the McAfee NSP product and its associated certification material. RC4 and MD5 are now considered obsolete for new TLS deployments due to known cryptographic weaknesses, so a current deployment should follow the vendor's supported modern TLS configuration guidance rather than treat this historical exam answer as a contemporary security recommendation. The TLS protocol's use of cipher suites and integrity mechanisms is described in the TLS 1.2 specification (RFC 5246). Current Trellix product documentation and security guidance are available through the Trellix Documentation Portal.

QUESTION NO: 11

McAfee recommends which of the following methods to cable the heartbeat connection of a sensor failover pair?

A. direct fiber connection with specified monitoring ports

B. direct copper connection using response ports

C. switched fiber connection

D. direct copper connection using failopen port

ANSWER: A

Explanation:

direct fiber connection with specified monitoring ports is the recommended heartbeat cabling method for a Network Security Platform Sensor failover pair. The heartbeat is the dedicated communication path through which the paired Sensors exchange availability and operational-status information. A direct physical fiber connection provides a controlled, point-to-point path between the appliances and avoids introducing intermediary network dependencies into the failover-health signal. The monitoring ports selected for this purpose must be the specific compatible ports identified for the Sensor model and failover deployment, with matching optics and correctly configured link settings. This design helps the failover pair detect loss of peer connectivity promptly and supports reliable role transition when a Sensor becomes unavailable. It also keeps heartbeat traffic separate from ordinary production switching and inspection traffic, which is important because the heartbeat link is part of the high-availability design rather than a general network connection. For current product and documentation resources, see the Trellix Network Security Platform product page and the Trellix documentation portal.