

MA0-101^{Q&As}

McAfee Certified Product Specialist - NSP

Pass McAfee MA0-101 Exam with 100% Guarantee

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

<https://www.leads4pass.com/ma0-101.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



QUESTION 1

Which port needs to be opened for Alert Channel communication between Sensor and Manager through a firewall?

- A. 8501
- B. 8502
- C. 8503
- D. 8555

Correct Answer: B

QUESTION 2

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

Correct Answer: A

QUESTION 3

Which mode needs to be set to redirect an unmanaged system to the guest portal?

- A. Audit
- B. Simulation
- C. Enforcement
- D. Prevention

Correct Answer: C

QUESTION 4

Which of the following should be applied to policies in both Inbound and Outbound directions?

- A. Policy rules
- B. Reconnaissance rules

C. Attack parameters

D. Rule sets

Correct Answer: D

QUESTION 5

_____ are a set of Access Control List (ACL) rules that define network access provided to a host, subject to Network Access Control.

A. Network Access Lists

B. Network Access Objects

C. Network Access Zones

D. Network Access Policy

Correct Answer: C

QUESTION 6

Which command can be issued on a Sensor to check the health of the Sensor?

A. show

B. show settings

C. status

D. check health

Correct Answer: C

QUESTION 7

What is the command to force the sensor out of Layer 2 Passthru mode?

A. Layer2 mode off

B. Layer2 mode on

C. Layer2 mode assert

D. Layer2 mode deassert

Correct Answer: D

QUESTION 8

Which of the following CLI commands will not cause an automatic reboot of the Sensor?

- A. resetconfig
- B. delete signatures
- C. factorydefaults
- D. deinstall

Correct Answer: D

QUESTION 9

Which server type needs to be configured as a requirement before the Quarantined user classes and Quarantined DHCP server(s) are configured?

- A. Integrated DHCP server
- B. Wildcard DNS server
- C. WINS server
- D. Portal server

Correct Answer: B

QUESTION 10

IPS Policies can be enforced at which of the following sensor nodes?

- A. Sensor name node only
- B. Sensor name and interface node only
- C. Sensor sub-interface node only
- D. Sensor name, interface and sub-interface node

Correct Answer: D

QUESTION 11

Identity Based Access Control cannot co-exist with which mode of NAC deployment on the same port?

- A. System Health-based NAC
- B. DHCP NAC

C. L2 and L3 Deployment modes

D. Mixed Deployment modes

Correct Answer: B

QUESTION 12

Which of the following actions can a Standby Manager of an MDR pair perform?

A. Modify sensor configuration

B. Policy configuration

C. Signature update

D. Configuration backup

Correct Answer: D

QUESTION 13

If the Health Level of the host cannot be determined, which of the following System Health Levels would be assigned?

A. Fair

B. Poor

C. Serious

D. Unknown

Correct Answer: D

QUESTION 14

Which of the following options is the best practice to use if you need to edit all attacks with a specific severity number within an IPS policy?

A. Use the Bulk Edit feature within the Policy Editor

B. Create and run the appropriate database query

C. Edit the attacks individually

D. Use the Bulk Edit feature within the Reconnaissance Editor

Correct Answer: A

QUESTION 15

A sensor is placed in-line and is dropping traffic. This situation demands an immediate removal of the sensor from the network to let traffic flow uninterrupted. Which option will you use to verify whether the issue is due to sensor configuration or network congestion?

- A. Layer2modeon
- B. Layer2 mode assert
- C. Layer2 mode deassert
- D. Layer2 mode off

Correct Answer: A

[MA0-101 Study Guide](#)

[MA0-101 Exam Questions](#)

[MA0-101 Braindumps](#)