

McAfee MA0-102

McAfee Certified Product Specialist- HIPs

Version: 4.0

QUESTION NO: 1

Which of the following policy categories are considered to be multi-slot policies? (Select the two that apply)

- A. Trusted Application
- B. IPS Rules
- C. Firewall Rules
- D. IPS Protection
- E. IPS Options

Answer: A,B

Explanation:

QUESTION NO: 2

Firewall client rules are created in Adaptive Mode using which of the following parameters?

- A. Per-user
- B. Per-process
- C. Per-application
- D. Per-signature

Answer: B

Explanation:

QUESTION NO: 3

Which of the following is the main log file for IPS?

- A. FireTray.log
- B. HipShield log
- C. HipMgtPlugin.log
- D. McTrayHip.log

Answer: B

Explanation:

QUESTION NO: 4

The option to select Create Exception upon an Intrusion Event will only be available if the IPS Rules Policy has been configured with which of the following?

- A. Adaptive Mode
- B. Learn Mode
- C. Create Exceptions
- D. Allow Client Rules

Answer: D

Explanation:

QUESTION NO: 5

What detail property includes the Local Time Zone value of a managed machine?

- A. Virus Scan Enterprise properties
- B. McAfee Agent properties
- C. Host Intrusion Prevention properties
- D. System Information properties

Answer: D

Explanation:

QUESTION NO: 6

Under which HIPs Policy category can IPS Engines be disabled for troubleshooting?

- A. IPS Options
- B. Firewall Rules
- C. Trusted Applications (All Platforms)
- D. Client UI (Windows)

Answer: D

Explanation:

QUESTION NO: 7

Which of the following is the HIPs executable for the HIPs Client UI?

- A. FireSvc.exe
- B. FireTray.exe

- C. McAfeeFire.exe
- D. Mfefire.exe

Answer: C

Explanation:

QUESTION NO: 8

Which of the following are used to create custom signatures? (Select the three that apply)

- A. Signature Builder
- B. Signature Creation Wizard
- C. Advanced Mode
- D. Standard Mode
- E. Expert Mode

Answer: B,C,D

Explanation:

QUESTION NO: 9

Which of the following is a supported browser for Host IPS and ePO? (Select the two that apply)

- A. Internet Explorer
- B. Firefox
- C. Safari
- D. Chrome
- E. Opera

Answer: A,B

Explanation:

QUESTION NO: 10

Which of the following server services is responsible for communication with the McAfee agent?

- A. Apache
- B. Tomcat
- C. SQL
- D. Event Parser

Answer: A

Explanation:

QUESTION NO: 11

Which of the following are the listed signature severity levels within HIPs? (Select the four that apply)

- A. High
- B. Major
- C. Medium
- D. Minor
- E. Low
- F. Informational

Answer: A,C,E,F

Explanation:

QUESTION NO: 12

Which of the following items can be found under the IPS Policy tab in the HIPs Client UI?

- A. IPS exceptions from ePO Policy
- B. Locally created IPS Client Rules
- C. Blocked Hosts
- D. Firewall traffic

Answer: B

Explanation:

QUESTION NO: 13

Which of the following options cannot be used to define a trusted network?

- A. Single Address
- B. Address Range
- C. Subnet Address
- D. Network Protocol

Answer: D