DUMPSBOSS.

McAfee Certified Product Specialist - HIPS

McAfee MA0-102

Version Demo

Total Demo Questions: 8

Total Premium Questions: 84

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A Firewall administrator is reviewing a state-table entry for a permitted UDP conversation. Which set of values is required to distinguish that conversation from another UDP conversation using the same local port?

A. Protocol, local address, and local port

B. Protocol, local address, local port, and remote address

C. Protocol, local address, local port, remote address, and remote port

D. Protocol, local port, and remote port

ANSWER: C

Explanation:

A state-table entry is identified by the complete communication tuple: **protocol, local address, local port, remote address, and remote port**. Including both endpoint addresses and ports distinguishes separate conversations that might use the same protocol and local port. A definition that omits the remote port or remote address could incorrectly treat different remote communications as the same flow.

QUESTION NO: 2

An administrator wants a corporate baseline policy to remain in effect while a smaller group receives additional Host IPS definitions without duplicating the baseline policy. Which policy categories support this multi-slot assignment behavior? (Select two)

A. Trusted Application

B. IPS Rules

C. Firewall Rules

D. IPS Protection

E. IPS Options

ANSWER: A B

Explanation:

Trusted Application and **IPS Rules** are multi-slot policy categories. Multiple applicable policies in these categories can be retained through the assignment hierarchy, which allows a baseline set of trusted application entries or IPS rules to be supplemented for a more specific group. Firewall Rules and the IPS protection and options categories do not provide this same layered multi-slot behavior; their effective settings are determined by the applicable assigned policy rather than by combining multiple policy slots.

QUESTION NO: 3

An administrator is using Host IPS Application Protection to reduce the ability of malicious code to modify critical host resources. Which resources are protected by the Shielding and Enveloping feature? (Select three)

A. Applications

B. Firewall traffic

C. System registry

D. Services

E. Repository content

ANSWER: A C D

Explanation:

Application Protection uses Shielding and Enveloping to lock down **applications**, the **system registry**, and **services** against malicious activity. This is host-level protection of applications and critical operating-system resources. Firewall traffic controls and repository content are managed through separate Host IPS and ePolicy Orchestrator functions.

QUESTION NO: 4

Which of the following are the accepted methods of creating exceptions? (Select the two that apply)

A. Evasion tool

B. ClientException utility

C. Manually

D. Adaptive Mode

E. Learn Mode

ANSWER: C D

Explanation:

“Manually” and “Adaptive Mode” are accepted methods for creating Host Intrusion Prevention System exceptions. An administrator can create an exception manually when the required behavior, application, process, or rule condition is already known. This approach provides deliberate, controlled policy configuration and is appropriate when administrators have verified that allowing the activity does not undermine the intended protection.

Adaptive Mode provides a monitored learning workflow for exception creation. In this mode, Host IPS observes activity that would otherwise be blocked or reported and enables the administrator to review and convert suitable observed behavior into exceptions. This is especially useful for identifying legitimate application behavior in an environment before enforcing a more restrictive policy. Exceptions created through either method are policy-based decisions: they are intended to accommodate known, authorized behavior while retaining protection for other activity.

For Host IPS product documentation and policy administration guidance, consult the Trellix Product Documentation portal and the Trellix Endpoint Security product information.

QUESTION NO: 5

Which of the following is the supported executable that is used to install HIPs for Windows?

A. McAfeeHIP_Install.msi

B. McAfeeHIPS_ClientSetup.exe

C. McAfeeHIP_ClienlSetup.msi

D. McAfeeHIP_Install.exe

ANSWER: B

Explanation:

`McAfeeHIPS_ClientSetup.exe` is the supported Windows client installer executable for McAfee Host Intrusion Prevention System (Host IPS). This executable is the deployment package intended to install the Host IPS client software on

managed Windows endpoints. It supports the installation workflow used by Host IPS deployments, including use through McAfee ePolicy Orchestrator (ePO) after the Host IPS package has been checked in to the repository, or for supported local installation scenarios. The name is significant: `HIPS` is the product abbreviation and `ClientSetup.exe` identifies the executable bootstrap installer for the endpoint client. The installer handles the prerequisite and package-installation process required to place the Host IPS client components on Windows, after which policy and configuration can be managed centrally. Administrators should obtain the package from the licensed product download/repository source that corresponds to their Host IPS version and platform, and should follow the applicable Host IPS product documentation for supported operating systems, upgrade paths, and deployment procedures. McAfee enterprise products and associated documentation are now maintained under Trellix; see the Trellix Product Documentation portal and the Trellix Support portal for current documentation and downloads.

QUESTION NO: 6

In order to locally install HIPs over a previously installed version, which of the following must be disabled?

A. Firewall

B. McAfee Agent Policy Enforcement

C. VSE On-Access Scanner

D. IPS Protection

ANSWER: A

Explanation:

Firewall must be disabled before performing a local, in-place installation of Host Intrusion Prevention System over an existing installation. The installed Host IPS firewall is a host-based, stateful filtering component that can continue to enforce its existing rules while the installer is attempting to stop, replace, and register Host IPS services and drivers. Temporarily disabling it avoids interference with the local upgrade process and helps ensure that the replacement components can be installed and initialized correctly. This is specifically a preparation step for a locally initiated installation over a prior Host IPS version; after the installation is complete and the endpoint has received the appropriate policy, firewall protection should be restored and verified. Administrators should also schedule the work in accordance with their organization's change-control process, because disabling the firewall temporarily changes the endpoint's network-protection posture. Trellix, the current successor for these product resources, provides its documentation portal at Trellix Product Documentation and product-support resources at Trellix Support.

QUESTION NO: 7

Which of the following types of signatures can be contained within an IPS Rules Policy? (Select the three that apply)

A. Host

B. Custom Host

C. Network

D. Custom Network

E. Digital

ANSWER: A B C

Explanation:

An IPS Rules Policy can contain **Host**, **Custom Host**, and **Network** signatures. Host signatures provide protection by monitoring and enforcing rules on activity occurring locally on the managed endpoint, such as operating-system, application, and process behavior. Custom Host signatures allow an administrator to define organization-specific host-level detection or prevention logic when the supplied signature content does not address a particular internal requirement. Network signatures

inspect network traffic associated with the endpoint and identify known attack patterns, protocol misuse, and other suspicious communications that can be detected through network-level analysis.

These signature categories are made available together in the IPS Rules Policy so that endpoint protection can apply both vendor-provided detection content and locally created host protections in a centrally managed policy. Administrators can enable, disable, configure, and assign the applicable signature rules through the management console, allowing protection to be tailored to the endpoint group, risk profile, and operational requirements. For product documentation and supported-management guidance, consult the Trellix Product Documentation portal and the Trellix Support portal.

QUESTION NO: 8

Which of the following is the HIPs policy that allows a generated listing of applications that are known to be safe and are allowed to perform any normal operation?

A. Trusted Applications Policy

B. Local Applications Policy

C. Safe Applications Policy

D. Host Application

ANSWER: A

Explanation:

Trusted Applications Policy is the HIPS policy used to maintain a list of executables that are explicitly trusted. Applications included in this generated trusted list are treated as safe by Host Intrusion Prevention System policy enforcement and can perform normal operations without being subjected to the restrictions that application-control rules might otherwise impose. This provides an efficient way to prevent known, approved business software from being interrupted while HIPS continues to monitor and control untrusted or unknown processes.

In ePolicy Orchestrator, the policy is centrally managed and distributed to HIPS-managed endpoints, allowing administrators to keep trusted-application treatment consistent across the environment. Trust can be established using application-identifying information such as the executable's file details or other supported criteria, so the policy is intended for software whose source and behavior have been validated by the organization. The generated listing described in the question is therefore specifically the trusted-applications mechanism, rather than a generic host or local application setting. For McAfee/Trellix product documentation and support resources, see the Trellix Knowledge Center and the Trellix Support portal.