Free Questions for Deep-Security-Professional by actualtestdumps

Shared by Mccarthy on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How is scan caching used in agentless implementations of Deep Security?

Options:

A- Scan caching maintains the Inclusions and Exclusions lists from the Malware Scan Configuration in memory to improve performance.

B- Scan caching manages resource usage by staggering the launch of malware scans to prevent scan storms

C- Scan caching is used in Agent-based installations only and is not supported in an agentless implementation.

D- Scan caching enhances the performance of the Deep Security Virtual Appliance in that files scanned for malware on a virtual machine that appear on other virtual machines may not need to be scanned again.

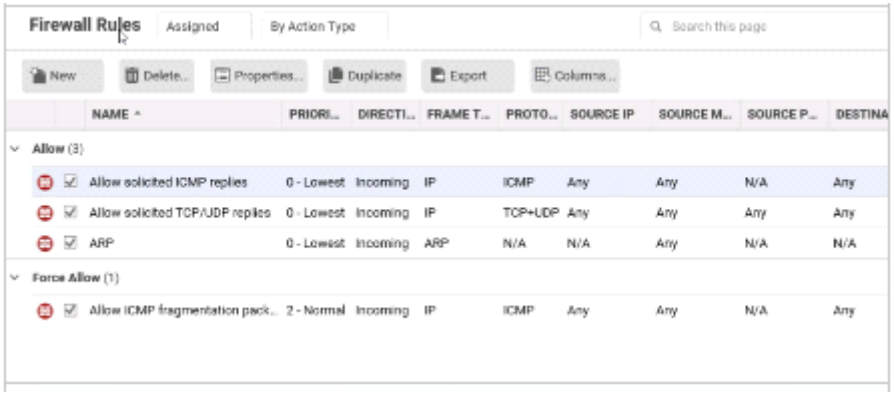
Answer:

D

Question 2

Question Type: MultipleChoice

While viewing the details of the Firewall Protection Module, as displayed in the exhibit, you note that a few rules have already been assigned. You try to disable these rules, but they can not be unassigned. Why can the displayed rules not be unassigned?



Options:

A- The rules displayed in the exhibit have been hard-coded with the details of the policy. These rules will automatically be assigned to all Firewall policies that are created and can not be unassigned.

B- The rules displayed in the exhibit have been assigned to the policy at the parent level. Rules assigned to a parent policy can not be unassigned at the child level.

C- The rules displayed in the exhibit were assigned to the policy automatically when a Recommendation Scan was run. Rules assigned through a Recommendation Scan can not be disabled once assigned.

D- The rules displayed in the exhibit can not be unassigned as the administrator currently logged into the Deep Security Manager Web console does not have the permissions necessary to unassign rules.

Answer:

B

Question 3

Question Type: MultipleChoice

Recommendation scans can detect applications and/or vulnerabilities on servers on the network. Which of the following Protection Modules make use of Recommendation scans?

Options:

A- Firewall, Application Control, and Integrity Monitoring

B- Intrusion Prevention, Firewall, Integrity Monitoring and Log Inspection

C- Log Inspection, Application Control, and Intrusion Prevention

D- Intrusion Prevention, Integrity Monitoring, and Log Inspection

Answer:

D

Explanation:

Recommendation Scans can suggest rules for the following Protection Modules:

* Intrusion Prevention

* Integrity Monitoring

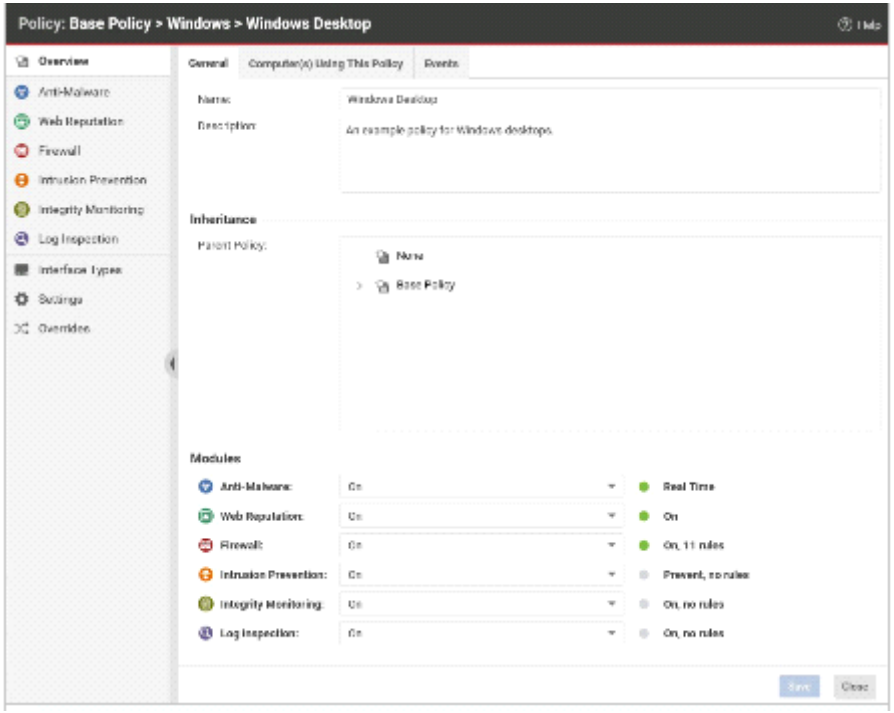
* Log Inspection

Explication: Study Guide - page (161)

Question 4

Question Type: **MultipleChoice**

When viewing the details for a policy, as displayed in the exhibit, you notice that the Application Control Protection Module is not available. In this example, why would this Protection Modules not be available?



Options:

A- The Application Control Protection Module has been disabled at the Base Policy level and is not displayed in the details for child policies.

B- The Application Control Protection Module is only supported on Linux computers, the policy details displayed are for Windows computers only.

C- An Activation Code for the Application Control Protection Module has not been pro-vided. Unlicensed Protection Modules will not be displayed.

D- The Application Control Protection Modules has not been enabled for this tenant.

Answer:

C

Explanation:

testing-the-deep-security-modules

Question 5

Question Type: MultipleChoice

Which of the following correctly identifies the order of the steps used by the Web Reputation Protection Module to determine if access to a web site should be allowed?

Options:

A- Checks the cache. 2. Checks the Deny list. 3. Checks the Approved list. 4. If not found in any of the above, retrieves the credibility score from Rating Server. 5. Evaluates the credibility score against the Security Level to determine if access to the web site should be allowed.

B- Checks the cache. 2. Checks the Approved list. 3. Checks the Deny list. 4. If not found in any of the above, retrieves the credibility score from the Rating Server. 5. Evaluates the credibility score against the Security Level to determine if access to the web site should be allowed.

C- Checks the Deny list. 2. Checks the Approved list. 3. Checks the cache. 4. If not found in any of the above, retrieves the credibility score from Rating Server. 5. Evaluates the credibility score against the Security Level to determine if access to the web site should be allowed.

D- Checks the Approved list. 2. Checks the Deny list. 3. Checks the cache. 4. If not found in any of the above, retrieves the credibility score from the Rating Server. 5. Evaluates the credibility score against the Security Level to determine if access to the web site should be allowed.

Answer:

D

Question 6

Question Type: **MultipleChoice**

Which of the following statements is false regarding Firewall rules using the Bypass action?

Options:

A- Applying a Firewall rule using the Bypass action to traffic in one direction automatically applies the same action to traffic in the other direction.

B- Firewall rules using the Bypass action do not generate log events.

C- Firewall rules using the Bypass action allow incoming traffic to skip both Firewall and Intrusion Prevention analysis.

D- Firewall rules using the Bypass action can be optimized, allowing traffic to flow as effi-ciently as if a Deep Security Agent was not there.

Answer:

A

Explanation:

Firewall rules using Bypass have the following noteworthy characteristics:

* Bypass skips both Firewall and Intrusion Prevention analysis.

* Since stateful inspection is for bypassed traffic, bypassing traffic in one direction does not automatically bypass the response in the other direction. As a result firewall rules using Bypass are always created in pairs, one for incoming traffic and another for outgoing.

* Firewall rules using Bypass will not be logged. This is not a configurable behavior.

* Some firewall rules using Bypass are optimized, in that traffic will flow as efficiently as if the Deep Security Agent/Deep Security Virtual Appliance was not there.

Explication: Study Guide - page (236)

Question 7

Question Type: MultipleChoice

Which Protection Modules can make use of a locally installed Smart Protection Server?

Options:

A- The Anti-Malware and Web Reputation Protection Modules can make use of the locally installed Smart Protection Server.

B- All Protection Modules can make use of the locally installed Smart Protection Server

C- Anti-Malware is the only Protection Modules that can use the locally installed Smart Protection Server.

D- The Anti-Malware, Web Reputation and Intrusion Prevention Protection Modules can make use of the locally installed Smart Protection Server.

Answer:

A

Explanation:

Smart Protection