



# Free Questions for Deep-Security- Professional

Shared by **Alvarado** on **13-09-2022**

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)



# Question 1

Question Type: MultipleChoice

Based on the Malware Scan Configuration displayed in the exhibit, which of the following statements is false.

The screenshot shows the 'Advanced Real-Time Scan Configuration' dialog box. The 'General' tab is active. The configuration is as follows:

- General Information:** Name: Advanced Real-Time Scan Configuration; Description: (empty); Scan Type: Real-time.
- Document Exploit Protection:**  Scan documents for exploits. Sub-options:  Scan for exploits against known critical vulnerabilities only;  Scan for exploits against known critical vulnerabilities and aggressive detection of unknown suspicious exploits.
- Predictive Machine Learning:**  Enable Predictive Machine Learning.
- Behavior Monitoring:**  Detect suspicious activity and unauthorized changes (incl. ransomware);  Back up and restore ransomware encrypted files.
- Spyware/Grayware:**  Enable spyware/grayware protection.
- IntelliTrap:**  Enable IntelliTrap.
- Process Memory Scan:**  Scan process memory for malware.

Buttons: OK, Cancel, Apply.

## Options:

- A- Any document files that display suspicious behavior will be submitted and executed in a sandbox environment on a Deep Discover Analyzer device.
- B- Deep Security Agents using this Malware Scan Configuration will not monitor for compromised Windows processes.
- C- Deep Security Agents will only be able to identify malware in files by using patterns downloaded from the Smart Protection Network.
- D- Internet access is required to properly enable the features identified in this configuration.

## Answer:

B

## Explanation:

Configure Malware Scan

---

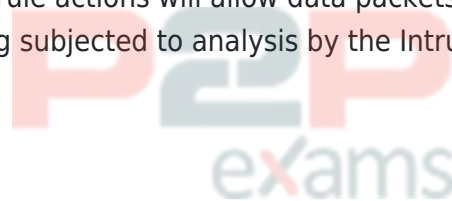
## Question 2

---

Question Type: MultipleChoice

---

Which of the following Firewall rule actions will allow data packets to pass through the Firewall Protection Module without being subjected to analysis by the Intrusion Prevention Protection Module?



### Options:

---

- A- Deny
- B- Bypass
- C- Allow
- D- Force Allow

### Answer:

---

B

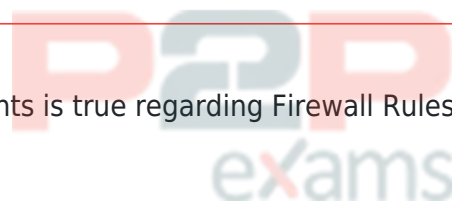
## Question 3

---

Question Type: MultipleChoice

---

Which of the following statements is true regarding Firewall Rules?



### Options:

---

- A- Firewall Rules applied to Policy supersede similar rules applied to individuals computers.
- B- When traffic is intercepted by the network filter, Firewall Rules in the policy are always applied before any other processing is done.
- C- Firewall Rules applied through a parent-level Policy cannot be unassigned in a child-level policy.
- D- Firewall Rules are always processed in the order in which they appear in the rule list, as displayed in the Deep Security manager Web console.

Answer:

---

C

## Question 4

---

Question Type: MultipleChoice

---

Which of the following statements is true regarding Intrusion Prevention protection?

Options:

- A- Intrusion Prevention protection can drop malicious packets but cannot reset the connection.
- B- Intrusion Prevention protection only works in conjunction with the Anti-Malware Protection Module.
- C- Intrusion Prevention protection can only work on computers where a Deep Security Agent is installed; agentless protection is not supported.
- D- Intrusion Prevention protection can drop or reset a connection.

Answer:

---

D

## Question 5

---

Question Type: MultipleChoice

---

What is the purpose of the override.properties file?

Options:

- A- This file is used to transfer policy settings from one installation of Deep Security Manager to another
- B- This file allows properties to be tested on Deep Security Manager without affecting the original configuration.
- C- This file contains the original out-of-the-box configuration properties for Deep Security Manager. This file is renamed to dsm.properties upon initialization of Deep Security Manager.
- D- This file allows Deep Security Agents to override enforced behavior by providing new policy configuration details.

Answer:

---

B

Explanation:

---

The properties specified in this configuration file override the properties specified in the dsm.properties file. This file can be created manually by a support engineer to modify product behavior without affecting the original configuration.

Explication: Study Guide - page (42)



## Question 6

---

Question Type: MultipleChoice

---

What is the purpose of the Deep Security Notifier?

Options:

---

- A- The Deep Security Notifier is a application in the Windows System Tray that displays the Status of Deep Security Manager during policy and software updates.
- B- The Deep Security Notifier is a server components that collects log entries from managed computers for delivery to a configured SIEM device.
- C- The Deep Security Notifier is a server component used in agentless configurations to allow Deep Security Manager to notify managed computers of pending updates.
- D- The Deep Security Notifier is a application in the Windows System Tray that communicates the state of Deep Security Agents and Relays to endpoint computers.

Answer:

---

D

Explanation:

---

The Deep Security Notifier is a Windows System Tray application which provides local notification when malware is detected or malicious URLs are blocked.

It may be installed separately on protected virtual machines, however the Anti-Malware Protection Module must be licensed and enabled on the virtual machine for the Deep Security Notifier to display information.

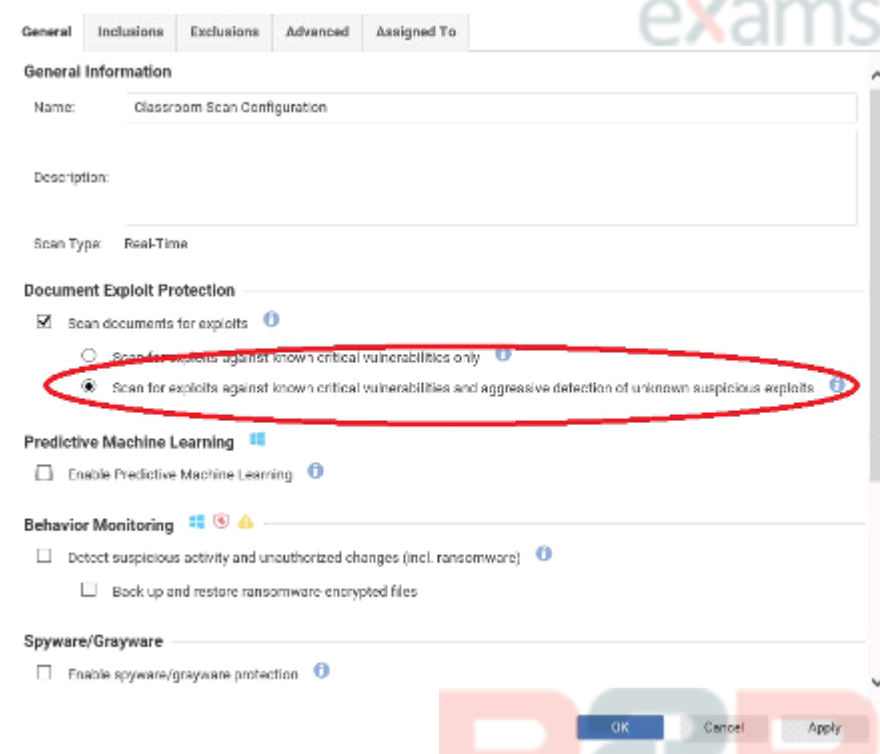
The Notifier displays pop-up user notifications when the Anti-Malware module begins a scan, or blocks malware or access to malicious web pages. The Notifier also provides a console utility that allows the user to view events.

Explication: Study Guide - page (442)

## Question 7

Question Type: MultipleChoice

Based on the configuration setting highlighted in the exhibit, what behavior can be expected during a malware scan?



The screenshot shows the configuration window for 'Classroom Scan Configuration'. The 'Document Exploit Protection' section has three radio button options:

- Scan documents for exploits
- Scan for exploits against known critical vulnerabilities only
- Scan for exploits against known critical vulnerabilities and aggressive detection of unknown suspicious exploits

The third option is highlighted with a red oval. Below this section are 'Predictive Machine Learning' and 'Behavior Monitoring' sections, both with disabled checkboxes. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

### Options:

- A- With the highlighted setting enabled, Deep Security Agents will scan files for known viruses and malware using patterns and any files deemed suspicious will be submitted to a configured Deep Discovery Analyzer for further analysis.
- B- With the highlighted setting enabled, Deep Security Agents will scan files for viruses and malware using supplementary aggressive detection pattern files.
- C- With the highlighted setting enabled, Deep Security Agents will scan files for unknown malware using Predictive Machine Learning.
- D- With the highlighted setting enabled, Deep Security Agents will scan files for known malware as well as newly encountered malware by accessing the Suspicious Objects List.

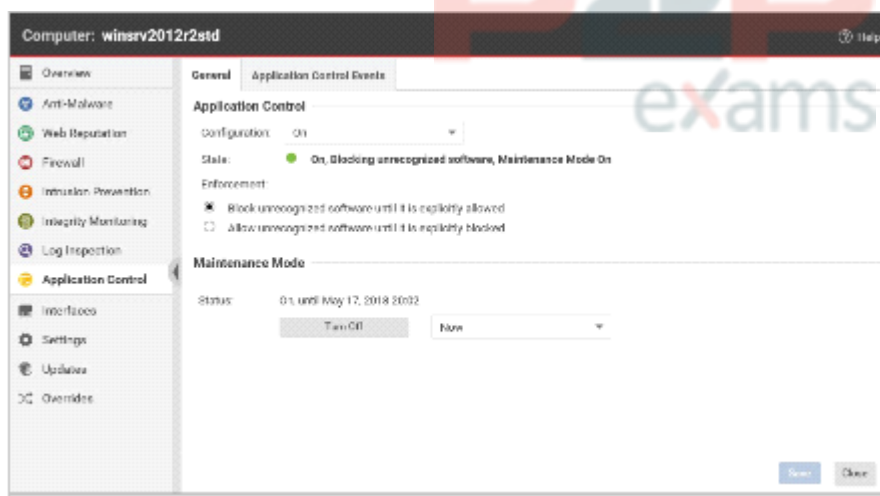
Answer:

D

## Question 8

Question Type: MultipleChoice

Based on the following exhibit, what behavior would you expect for the Application Control Protection Module?



Options:

- A- Since this computer is in Maintenance Mode, updates to the Application Control Protection Module will be applied.
- B- Since this computer is in Maintenance Mode, new or changed software will be automatically added to the list of Allowed software in the currently active ruleset.
- C- Since this computer is in Maintenance Mode, Application Control will allow any Blocked software to temporarily run
- D- Since this computer is in Maintenance Mode, Application Control will ignore any Blocked software in the currently active ruleset.

Answer:

A

## Question 9

Question Type: MultipleChoice

The Security Level for Web Reputation in a policy is set to High. A server assigned this policy attempts to access a Web site with a credibility score of 78.

What is the result?

Options:

---

- A- The Deep Security Agent allows access to the Web site, and logs the connection attempt as an Event.
- B- The Deep Security Agent allows access as the credibility score for the Web site is above the allowed threshold.
- C- The Deep Security Agent blocks access as the credibility score for the Web site is below the allowed threshold. An error page is displayed in the Web browser.
- D- The Deep Security Agent displays a warning message as the site is unrated.

Answer:

---

C

## Question 10

---

Question Type: MultipleChoice

---

Which of the following statements is true regarding software inventories used as part of the Application Control Protection Module?

Options:

---

- A- Disable the Application Control Protection Module when installing software upgrades, otherwise, the new software will be prevented from installing.
- B- An administrator can view the list of allowed software in the inventory from the De-tails tab for each individual Computer.
- C- An administrator can share the inventory of allowed software with other computers protected by Deep Security Agents, by copying the inventory database file (ac.db) from the source computer.
- D- When an administrator allows software that would be otherwise blocked by the En-forcement Mode, it isn't added to the inventory of approved software. Instead, it is added to that computer's white list.

Answer:

---



D



To Get Premium Files for Deep-Security-  
Professional Visit

<https://www.p2pexams.com/products/deep-security-professional>



For More Free Questions Visit

<https://www.p2pexams.com/trend/pdf/deep-security-professional>

