Trend

DEEP-SECURITY-PROFESSIONAL Exam

Trend Micro Certified Professional for Deep Security

Questions & Answers
Demo

Version: 4.0

Question: 1

Multiple Application Control Events are being displayed in Deep Security after a series of ap-plication updates and the administrator would like to reset Application Control. How can this be done?

A. On the Deep Security Agent computer, type the following command to reset Application Control: dsa_control -r
B. Click "Clear All" on the Actions tab in the Deep Security Manager Web console to reset the list of Application Control events.
C. Application Control can be reset by disabling the Protection Module, then enabling it once again. This will cause local rulesets to be rebuilt.
D. Application Control can not be reset.

Answer: C

Explanation:

Question: 2

The Firewall Protection Module is enabled on a server through the computer details. What is default behavior of the Firewall if no rules are yet applied?

A. All traffic is permitted through the firewall until either a Deny or Allow rule is assigned.
B. A collection of default rules will automatically be assigned when the Firewall Protection Module is enabled.
C. All traffic is blocked by the firewall until an Allow rule is assigned.
D. All traffic is passed through the Firewall using a Bypass rule

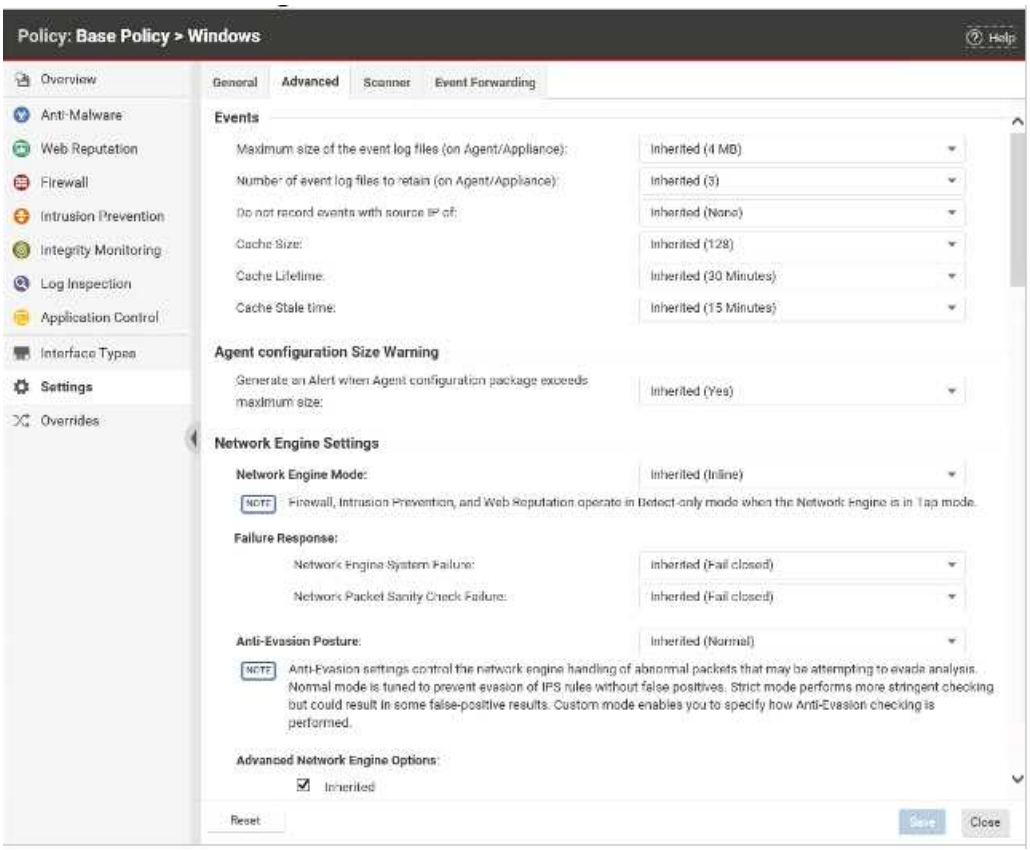
Answer: B

Explanation:

Deep Security provides a set of Firewall rules that can be applied to policies or directly to a com-puter. These default rules provide coverage for typical scenarios.
Set up the Deep Security firewall
Explication: Study Guide - page (219)

Question: 3

The details of a policy are displayed in the exhibit. Based on these details, which of the following statements is true?



A. The credibility scores for visited web sites will be cached. If access to the web site is re-quested again within 30 minutes, its credibility score will be retrieved from the cache instead of the configured Smart Protection source.
B. Packets failing the Network Packet Sanity Check will still be allowed to pass through the network engine.
C. Any events generated by computers within your corporate network, as defined by an IP address range, will be ignored
D. Live packet streams coming through the network engine will be replicated and all traffic analysis will be performed on the replicated stream

Answer: A

Explanation:

Question: 4

The Intrusion Prevention Protection Module is enabled, but the traffic it is trying to analyze is encrypted through https. How is it possible for the Intrusion Prevention Protection Module to monitor this encrypted traffic against the assigned rules?

A. It is possible to monitor the https traffic by creating an SSL Configuration. Creating a new SSL Configuration will make the key information needed to decrypt the traffic available to the Deep Security Agent.
B. The Intrusion Prevention Protection Module is not able to analyze encrypted https traffic.

C. The Intrusion Prevention Protection Module can only analyze https traffic originating from other servers hosting a Deep Security Agent.
D. The Intrusion Prevention Protection Module can analyze https traffic if the public cer-tificate of the originating server is imported into the certificate store on the Deep Secu-rity Agent computer.

Answer: A

Explanation:

inrusion-prevention-ssl-traffic

Question: 5

Which of following statements best describes Machine Learning in Deep Security?

A. Machine Learning is malware detection technique in which features of an executable file are compared against a cloud-based learning model to determine the probability of the file being malware.
B. Machine Learning is a malware detection technique in which files are scanned based on the true file type as determined by the file content, not the extension.
C. Machine Learning is a malware detection technique in which the Deep Security Agent monitors process memory in real time and once a process is deemed to be suspicious, Deep Security will perform additional checks with the Smart Protection Network to determine if this is a known good process.
D. Machine Learning is malware detection technique in which processes on the protected computer are monitored for actions that are not typically performed by a given process.

Answer: A

Explanation:

Predictive Machine Learning