# IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

**Exam** : **Deep Security Professional**

**Title** : Trend Micro Certified Professional for Deep Security Exam

**Version** : DEMO

1.How does Smart Scan vary from conventional pattern-based anti-malware scanning?
A. Smart Scan improves the capture rate for malware scanning by sending features of suspicious files to an cloud-based server where the features are compared to known malware samples.
B. Smart Scan shifts much of the malware scanning functionality to an external Smart Protection Server.
C. Smart Scan is performed in real time, where conventional scanning must be triggered manually, or run on a schedule.
D. Smart Scan identifies files to be scanned based on the content of the file, not the exten-sion.
**Answer:** B
**Explanation:**
Advantages of the Smart Scan pattern over the conventional pattern protection in OfficeScan (OSCE)

2.The Intrusion Prevention Protection Module is enabled and a Recommendation Scan is run to identify vulnerabilities on a Windows Server 2016 computer.
How can you insure that the list of recommendations is always kept up to date?
A. Disabling, then re-enabling the Intrusion Prevention Protection Module will trigger a new Recommendation Scan to be run. New rules will be included in the results of this new scan.
B. Recommendation Scans are only able to suggest Intrusion Prevention rules when the Protection Module is initially enabled.
C. Enable "Ongoing Scans" to run a recommendation scan on a regular basis. This will identify new Intrusion Prevention rules to be applied.
D. New rules are configured to be automatically sent to Deep Security Agents when Rec-ommendation Scans are run.
**Answer:** C

3.New servers are added to the Computers list in Deep Security Manager Web config by running a Discover operation.
What behavior can you expect for newly discovered computers?
A. Any servers discovered in the selected Active Directory branch hosting a Deep Security Agent will be added to the Computers list.
B. Any servers within the IP address range hosting a Deep Security Agent will be added to the Computers list.
C. Any servers within the IP address range that are hosting Deep Security Agents will be added to the Computers list and will be automatically activated.
D. Any servers within the IP address range will be added to the Computers list, regardless of whether they are hosting a Deep Security Agent or not.
**Answer:** B
**Explanation:**
When running a Discovery operation with Automatically Resolve IPs to hostnames enabled, it is possible that the discovery operation will find hostnames where Deep Security Manager can not.
Discovery is able to fall back to using a WINS query or NetBIOS broadcast to resolve the hostname in addition to DNS. Deep Security Manager only supports hostname lookup via DNS.
• Computers identified with this method can be automatically assigned a group, but not a policy.
• Agent software found on those computers will NOT be automatically activated.
• If a computer is listed through other detection methods, it will NOT be listed in the results of this search.

Study Guide - pages (345, 80)

4.Which of the following statements is true regarding Intrusion Prevention rules?
A. Intrusion Prevention rules can block unrecognized software from executing.
B. Intrusion Prevention rules check for the IP addresses of known malicious senders within a packet
C. Intrusion Prevention rules can detect or block traffic associated with specific applications, such as Skype or file-sharing utilities.
D. Intrusion Prevention rules monitor the system for changes to a baseline configuration.
**Answer:** C

5.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)