Vendor: Symantec

Exam Code: ST0-134

Exam Name: Symantec EndPoint Protection 12.1 Technical Assessment

Version: Demo

QUESTION 1
A financial company enforces a security policy that prevents banking system workstations from connecting to the Internet. Which Symantec Endpoint Protection technology is ineffective on this company's workstations?

A. Insight
B. Intrusion Prevention
C. Network Threat Protection
D. Browser Intrusion Prevention

Correct Answer: A

QUESTION 2
In addition to performance improvements, which two benefits does Insight provide? (Select two.)

A. reputation scoring for documents
B. zero-day threat detection
C. protection against malicious java scripts
D. false positive mitigation
E. blocking of malicious websites

Correct Answer: BD

QUESTION 3
Which Symantec Endpoint Protection defense mechanism provides protection against threats that propagate from system to system through the use of autorun.inf files?

A. Application and Device Control
B. SONAR
C. TruScan
D. Host Integrity

Correct Answer: A

QUESTION 4
Which protection technology can detect botnet command and control traffic generated on the Symantec Endpoint Protection client machine?

A. Insight
B. SONAR
C. Risk Tracer
D. Intrusion Prevention

Correct Answer: D

QUESTION 5
Which technology can prevent an unknown executable from being downloaded through a browser session?

A. Browser Intrusion Prevention
B. Download Insight
C. Application Control
D. SONAR

Correct Answer: B

QUESTION 6
Which Symantec Endpoint Protection technology blocks a downloaded program from installing browser plugins?

A. Intrusion Prevention
B. SONAR
C. Application and Device Control
D. Tamper Protection

Correct Answer: C

QUESTION 7
Which protection engine should be enabled to drop malicious vulnerability scans against a client system?

A. SONAR
B. Intrusion Prevention
C. Tamper Protection
D. Application and Device Control

Correct Answer: B

QUESTION 8
What is the file scan workflow order when Shared Insight Cache and reputation are enabled?

A. Symantec Insight > Shared Insight Cache server > local client Insight cache
B. local client Insight cache > Shared Insight Cache server > Symantec Insight
C. Shared Insight Cache server > local client Insight cache > Symantec Insight
D. local client Insight cache > Symantec Insight > Shared Insight Cache server

Correct Answer: B

QUESTION 9
What is a function of Symantec Insight?

A. provides reputation ratings for structured data
B. enhances the capability of Group Update Providers (GUP)
C. increases the efficiency and effectiveness of LiveUpdate
D. provides reputation ratings for binary executables

Correct Answer: D

QUESTION 10
Which Symantec Endpoint Protection component enables access to data through ad-hoc reports and charts with pivot tables?

A. Symantec Protection Center
B. Shared Insight Cache Server
C. Symantec Endpoint Protection Manager
D. IT Analytics

Correct Answer: D

QUESTION 11
Which Symantec Endpoint Protection Management (SEPM) database option is the default for deployments of fewer than 1,000 clients?

A. Embedded Using the Sybase SQL Anywhere database that comes with the product

B. On SEPM Installing Microsoft SQL on the same server as the SEPM
C. External to SEPM Using a preexisting Microsoft SQL server in the environment
D. Embedded Using the Microsoft SQL database that comes with the product

Correct Answer: A

QUESTION 12
Which two items are stored in the Symantec Endpoint Protection database? (Select two.)

A. Device Hardware IDs
B. User Defined Scans
C. Symantec Endpoint Protection Client for Linux
D. Symantec Endpoint Protection Client for Macintosh
E. Active Directory Synced Logon Credentials

Correct Answer: AD

QUESTION 13
Which task should an administrator perform to troubleshoot operation of the Symantec Endpoint Protection embedded database?

A. verify that dbsrv11.exe is listening on port 2638
B. check whether the MSSQLSERVER service is running
C. verify the sqlserver.exe service is running on port 1433
D. check the database transaction logs in X\Program Files\Microsoft SQL server

Correct Answer: A

QUESTION 14
What is a function of the Symantec Endpoint Protection client?

A. uploads logs to the Shared Insight Cache
B. sends and receives application reputation ratings from LiveUpdate
C. downloads virus content updates from Symantec Insight
D. provides a Lotus Notes email scanner

Correct Answer: D

QUESTION 15
Which option is unavailable in the Symantec Endpoint Protection console Run a command on the group menu item?

A. Disable SONAR
B. Scan
C. Disable Network Threat Protection
D. Update content and scan

Correct Answer: A

QUESTION 16
Which object in the Symantec Endpoint Protection Manager console describes the most granular level to which a policy can be assigned?

A. Group
B. Computer
C. User
D. Client

Correct Answer: A

QUESTION 17
Where can an administrator obtain the Sylink.xml file?

A. C\Program Files\Symantec\Symantec Endpoint Protection\ folder on the client
B. C\Program Files\Symantec\Symantec Endpoint Protection\Manager\data\inbox\agent\ folder on the Symantec Endpoint Protection Manager
C. by selecting the client group and exporting the communication settings in the Symantec Endpoint Protection Manager Console
D. by selecting the location and exporting the communication settings in the Symantec Endpoint Protection Manager Console

Correct Answer: C

QUESTION 18
An administrator edited a firewall policy from the Clients > Policies tab.? Later, the administrator is unable to find the modified policy under the Policies > Firewall policies list.
What is the likely cause?

A. The administrator has set the policy to shared.
B. The administrator has set the policy to non-shared.
C. The administrator failed to save the policy.
D. The policy failed to deploy.

Correct Answer: B

QUESTION 19
An administrator is unable to delete a location. What is the likely cause?

A. The location currently contains clients.
B. Criteria is defined within the location.
C. The administrator has client control enabled.
D. The location is currently assigned as the default location.

Correct Answer: D

QUESTION 20
Which two are policy types within the Symantec Endpoint Protection Manager? (Select two.)

A. Exceptions
B. Host Protection
C. Shared Insight
D. Intrusion Prevention
E. Process Control

Correct Answer: AD

QUESTION 21
What is a characteristic of a Symantec Endpoint Protection (SEP) domain?

A. Each domain has its own management server and database.
B. Every administrator from one domain can view data in other domains.
C. Data for each domain is stored in its own separate SEP database.
D. Domains share the same management server and database.

Correct Answer: D

QUESTION 22
An organization employs laptop users who travel frequently. The organization needs to acquire log data from these Symantec Endpoint Protection clients periodically. This must happen without the use of a VPN. Internet routable traffic should be allowed to and from which component?

A. Group Update Provider (GUP)
B. LiveUpdate Administrator Server (LUA)
C. Symantec Endpoint Protection Manager (SEPM)
D. IT Analytics Server (ITA)

Correct Answer: C

QUESTION 23
An administrator is responsible for the Symantec Endpoint Protection architecture of a large, multi-national company with three regionalized data centers. The administrator needs to collect data fromclients; however, the collected data must stay in the the local regional data center. Communication between the regional data centers is allowed 20 hours a day. How should the administrator architect this organization?

A. set up 3 domains
B. set up 3 sites
C. set up 3 locations
D. set up 3 groups

Correct Answer: B

QUESTION 24
A Symantec Endpoint Protection (SEP) Administrator is designing a new SEP architecture to ensure that clients continually maintain a current set of content updates. The criteria listed below must be considered.

1. Client systems are located in a single physical site where they are commonly offline for up to 2 weeks at a time
2. The Site consists of approximately 500 clients
3. Content Updates must be as current as possible
4. The embedded database must be used for the Symantec Endpoint Protection Manager Which content update methodology minimizes the impact to the external Internet connection?

A. deploy an Internal LiveUpdate Administrator (LUA) and define the LiveUpdate Policy so the clients get their updates from the LUA
B. change the product defaults to define content revisions to 42 and configure the LiveUpdate Policy so the clients get their updates from the Symantec Endpoint Protection Manager
C. configure the Live Update Policy so the clients get their updates from a public Symantec LiveUpdate server
D. change the product defaults to define content revisions to 14 and configure the LiveUpdate Policy so the clients get their updates from a Group Update Provider (GUP)

Correct Answer: B

QUESTION 25
An administrator is designing a new single site Symantec Endpoint Protection environment. Due to perimeter firewall bandwidth restrictions, the design needs to minimize the amount of traffic from content passing through the firewall. Which source must the administrator avoid using?

A. Symantec Endpoint Protection Manager
B. LiveUpdate Administrator (LUA)
C. Group Update Provider (GUP)
D. Shared Insight Cache (SIC)

Correct Answer: B

QUESTION 26
A company plans to install six Symantec Endpoint Protection Managers (SEPMs) spread evenly across two sites. The administrator needs to direct replication activity to SEPM3 server in Site 1 and SEPM4 in Site 2. Which two actions should the administrator take to direct replication activity to SEPM3 and SEPM4? (Select two.)

A. install SEPM3 and SEPM4 after the other SEPMs
B. install the SQL Server databases on SEPM3 and SEPM4
C. ensure SEPM3 and SEPM4 are defined as the top priority server in the Site Settings
D. ensure SEPM3 and SEPM4 are defined as remote servers in the replication partner configuration install IT Analytics on SEPM3 and SEPM4

Correct Answer: CD

QUESTION 27
A multi-national company has two Symantec Endpoint Protection Managers and one database. An office in Germany with 50 clients needs Symantec Endpoint Protection (SEP). German regulations require the client's data remain localized for use in Germany. Which SEP components should the administrator install in Germany?

A. SEP client software with a dedicated Group Update Provider (GUP)
B. SEP client software with an Internal LiveUpdate server
C. A second isolated SEP site with SEP client software
D. A second replicated SEP site with SEP client software

Correct Answer: C

QUESTION 28
In Symantec Endpoint Protection 12.1 Enterprise Edition, what happens when the license expires?

A. LiveUpdate stops.
B. Group Update Providers (GUP) stop.
C. Symantec Insight is disabled.
D. Content updates continue.

Correct Answer: D

QUESTION 29
An administrator receives a browser certificate warning when accessing the Symantec Endpoint Protection Manager (SEPM) Web console. Where can the administrator obtain the certificate?

A. SEPM console Licenses section
B. Admin > Servers > Configure SecureID Authentication
C. SEPM console Admin Tasks
D. SEPM Web Access

Correct Answer: D

QUESTION 30
An administrator needs to configure Secure Socket Layer (SSL) communication for clients. In the httpd.conf file, located on the Symantec Endpoint Protection Manager (SEPM), the administrator removes the hashmark (#) from the text string displayed below. #Include conf/ssl/sslForcClients.conf Which two tasks must the administrator perform to complete the SSL configuration? (Select two.)

A. edit site.properties and change the port to 443
B. restart the Symantec Endpoint Protection Manager Webserver service
C. change the default certificates on the SEPM and reboot

D. change the Management Server List and enable HTTPs
E. change the port in Clients > Group > Policies > Settings > Communication Settings and force the clients to reconnect

Correct Answer: BD

QUESTION 31
Which two items should an administrator enter in the License Activation Wizard to activate a license? (Select two.)

A. password for the Symantec Licensing Site
B. purchase order number
C. serial number
D. Symantec License file
E. credit card number

Correct Answer: CD

QUESTION 32
A client is unable to communicate with the Symantec Endpoint Protection Manager (SEPM) Server. The administrator decides to use the Communications Update Package Deployment in the Client Deployment Wizard. Which two options are available using the Communications Update Package Deployment? (Select two.)

A. Policy Mode
B. SEPM Server Migration
C. Client Reboot
D. Content Update
E. Password Protection

Correct Answer: AE

QUESTION 33
Which two criteria should an administrator use when defining Location Awareness for the Symantec Endpoint Protection (SEP) client? (Select two.)

A. NIC description
B. SEP domain
C. geographic location
D. WINS server
E. Network Speed

Correct Answer: AD

QUESTION 34
A managed service provider (MSP) is managing Symantec Endpoint Protection for a number of independent companies. Each company has administrators who will log in from time to time to add new clients. Administrators must be prevented from seeing the existence of other companies in the console. What should an administrator create for each independent company?

A. Domain
B. Location
C. Group
D. Site

Correct Answer: A

QUESTION 35

What are two supported Symantec Endpoint Protection Manager authentication types? (Select two.)

A. Microsoft Active Directory
B. MS-CHAP
C. RSA SecurID
D. Biometrics
E. Network Access Control

Correct Answer: AC

QUESTION 36
In which two areas can host groups be used? (Select two.)

A. Application and Device Control
B. Firewall
C. Locations
D. IPS
E. Download Insight

Correct Answer: BD

QUESTION 37
Which tool should an administrator use to discover and deploy the Symantec Endpoint Protection client to new computers?

A. Unmanaged Detector
B. Client Deployment Wizard
C. Communication Update Package Deployment
D. Symantec Endpoint Discovery Tool

Correct Answer: B

QUESTION 38
A Symantec Endpoint Protection (SEP) administrator is remotely deploying SEP clients, but the clients are failing to install on Windows XP. What are two possible reasons for preventing installation? (Select two.)

A. Windows firewall is enabled.
B. Internet Connection firewall is disabled.
C. Administrative file shares are enabled.
D. Simple file sharing is enabled.
E. Clients are configured for DHCP.

Correct Answer: AD

QUESTION 39
A large software company runs a small engineering department that is remotely located over a slow WAN connection. Which option should the company use to install an exported Symantec Endpoint Protection (SEP) package to the remote site using the smallest amount of network bandwidth?

A. a SEP package using Basic content
B. a SEP package using a policy defined Single Group Update Provider (GUP)
C. a SEP package using a policy defined Multiple Group Update Provider (GUP) list
D. a SEP package using the Install Packages tab

Correct Answer: A

QUESTION 40

A company deploys Symantec Endpoint Protection client to its sales staff who travel across the country. Which deployment method should the company use to notify its sales staff to install the client?

A. Push mode
B. Client Deployment Wizard
C. Pull mode
D. Unmanaged Detector

Correct Answer: B

QUESTION 41
Which systems can be identified for deployment using the Find Computers option when using the Client Deployment Wizard?

A. Mac OS
B. Linux
C. Windows 2000
D. Windows 2008 - 64bit OS

Correct Answer: D

QUESTION 42
A client is unable to connect to the Symantec Endpoint Protection Manager (SEPM) to retrieve the latest policy. Which action should an administrator take to identify when the client last connected to the SEPM?

A. view the Control log on the Client
B. view the System log on the Client
C. view the Computer Status > Client Online Status report on the SEPM
D. .view the Computer Status > Client With Latest Policy report on the SEPM

Correct Answer: B

QUESTION 43
A company deploys Symantec Endpoint Protection (SEP) to 50 virtual machines running on a single ESXi host. Which configuration change can the administrator make to minimize sudden IOPS impact on the ESXi server while each SEP endpoint communicates with the Symantec Endpoint Protection Manager?

A. increase Download Insight sensitivity level
B. reduce the heartbeat interval
C. increase download randomization window
D. reduce number of content revisions to keep

Correct Answer: C

QUESTION 44
Where in the Symantec Endpoint Protection (SEP) management console will a SEP administrator find the option to allow all users to enable and disable the client firewall?

A. Client User Interface Control Settings
B. Overview in Firewall Policy
C. Settings in Intrusion Prevention Polic
D. System Lockdown in Group Policy

Correct Answer: A

QUESTION 45
A company has 10,000 Symantec Endpoint Protection (SEP) clients deployed using two Symantec Endpoint Protection Managers (SEPMs). Which configuration is recommended to ensure that each SEPM

is able to effectively handle the communications load with the SEP clients?

A. Push mode
B. Client control mode
C. Server control mode
D. Pull mode

Correct Answer: D

QUESTION 46
A Symantec Endpoint Protection (SEP) client uses a management server list with three management servers in the priority 1 list. Which mechanism does the SEP client use to select an alternate management server if the currently selected management server is unavailable?

A. The client chooses another server in the list randomly.
B. The client chooses a server based on the lowest server load.
C. The client chooses a server with the next highest IP address.
D. The client chooses the next server alphabetically by server name.

Correct Answer: A

QUESTION 47
A system running Symantec Endpoint Protection is assigned to a group with client user interface control settings set to mixed mode with Auto-Protect options set to Client. The user on the system is unable to turn off Auto-Protect. What is the likely cause of this problem?

A. Tamper protection is enabled.
B. System Lockdown is enabled.
C. Application and Device Control is configured.
D. The padlock on the enable Auto-Protect option is locked.

Correct Answer: D

QUESTION 48
Which action does the Shared Insight Cache (SIC) server take when the whitelist reaches maximum capacity?

A. The SIC server allocates additional memory for the whitelist as needed.
B. The SIC server will start writing the cache to disk.
C. The SIC server will remove the least recently used items based on the prune size.
D. The SIC server will remove items with the fewest number of votes.

Correct Answer: C

QUESTION 49
Which feature reduces the impact of Auto-Protect on a virtual client guest operating system?

A. Network Shared Insight Cache
B. Virtual Image Exception
C. Scan Randomization
D. Virtual Shared Insight Cache

Correct Answer: B

QUESTION 50
Which policy should an administrator modify to enable Virtual Image Exception (VIE) functionality?

A. Host Integrity Policy

B. Virus and Spyware Protection Policy
C. Exceptions Policy
D. Application and Device Control Policy

Correct Answer: B

QUESTION 51
Multiple Windows virtual clients running on an ESX server need to be scanned daily by a scheduled scan. Which feature should an administrator use to improve scan performance on the clients?

A. Virtual Image exceptions
B. Centralized Scan exceptions
C. Download Insight
D. Tamper Protection

Correct Answer: A

QUESTION 52
The LiveUpdate Download Schedule is set to the default on the Symantec Endpoint Protection Manager (SEPM). How many content revisions must the SEPM keep to ensure clients that check in to the SEPM every 10 days receive xdelta content packages instead of full content packages?

A. 10
B. 20
C. 30
D. 60

Correct Answer: C

QUESTION 53
Which client log shows that a client is downloading content from its designated source?

A. Risk Log
B. System Log
C. SesmLu.log
D. Log.LiveUpdate

Correct Answer: B

QUESTION 54
Which setting can an administrator configure in the LiveUpdate Policy?

A. specific content revision to download from a Group Update Provider (GUP)
B. specific content policies to download
C. Linux Settings
D. frequency to download content

Correct Answer: D

QUESTION 55
Which two sources can a Macintosh client use to download content? (Select two.)

A. Symantec Endpoint Protection Manager
B. Group Update Provider (GUP)
C. Internal LiveUpdate server
D. Default Management server
E. Symantec LiveUpdate server

Correct Answer: CE

QUESTION 56
Which ports on the company firewall must an administrator open to avoid problems when connecting to Symantec Public LiveUpdate servers?

A. 25, 80, and 2967
B. 2967, 8014, and 8443
C. 21, 443, and 2967
D. 21, 80, and 443

Correct Answer: D

QUESTION 57
A company has a small number of systems in their Symantec Endpoint Protection Manager (SEPM) group with federal mandates that AntiVirus definitions undergo a two week testing period. After being loaded on the client, the tested virus definitions must remain unchanged on the client systems until the next set of virus definitions have completed testing. All other clients must remain operational on the most recent definition sets. An internal LiveUpdate Server has been considered as too expensive to be a solution for this company. What should be modified on the SEPM to meet this mandate?

A. The LiveUpdate Settings policy for this group should be modified to use an Explicit Group Update Provider.
B. The LiveUpdate Content policy for this group should be modified to use a specific definition revision.
C. The SEPM site LiveUpdate settings should be modified so the Number of content revisions to keep is set to 1.
D. The SEPM site LiveUpdate settings should be modified so the Number of content revisions to keep is set to 14.

Correct Answer: B

QUESTION 58
An exception needs to be created for a file named "RunMe.exe" in a user's Windows 7 "My Documents" folder. The user's login name is Bob. Which method should be used?

A. create a file exception for "RunMe.exe" with a Prefix Variable of [USERNAME]
B. create a file exception for "[Drive]\Users\Bob\My Documents\RunMe.exe"
C. create a file exception for "*\RunMe.exe"
D. create a file exception for "RunMe.exe" with a Prefix Variable of %USERPROFILE%

Correct Answer: B

QUESTION 59
Which exception type can be configured?

A. Parent Process
B. Browser Object
C. MAC Address
D. Trusted Web Domain

Correct Answer: D

QUESTION 60
An administrator needs to add an Application Exception. When the administrator accesses the Application Exception dialog window, applications fail to appear. What is the likely problem?

A. The Learn applications that run on the client computers setting is disabled.
B. The client computers already have exclusions for the applications.

C. The Symantec Endpoint Protection Manager is installed on a Domain Controller.
D. The clients are in a trusted Symantec Endpoint Protection domain.

Correct Answer: A

QUESTION 61
A company uses a remote administration tool that is detected and quarantined by Symantec Endpoint Protection (SEP). Which step can an administrator perform to continue using the remote administration tool without detection by SEP?

A. create a Tamper Protect exception for the tool
B. create an Application to Monitor exception for the tool
C. create a Known Risk exception for the tool
D. create a SONAR exception for the tool

Correct Answer: C

QUESTION 62
A company receives a high number of reports from users that files being downloaded from internal web servers are blocked. The Symantec Endpoint Protection administrator verifies that the Automatically trust any file downloaded from an intranet website option is enabled. Which configuration can cause Insight to block the files being downloaded from the internal web servers?

A. Intrusion Prevention is disabled.
B. Local intranet zone is configured incorrectly on the Windows clients browser settings.
C. Local intranet zone is configured incorrectly on the Mac clients browser settings.
D. Virus and Spyware Definitions are out of date.

Correct Answer: B

QUESTION 63
Which action should an administrator take to prevent users from using Windows Security Center?

A. set Disable antivirus alert within Windows Security Center to Disable
B. set Disable antivirus alert within Windows Security Center to Never
C. set Disable Windows Security Center to Disable
D. set Disable Windows Security Center to Always

Correct Answer: D

QUESTION 64
An administrator is reviewing an Infected Clients Report and notices that a client repeatedly shows the same malware detection. Although the client remediates the files, the infection continues to display in the logs. Which two functions should be enabled to automate enhanced remediation of a detected threat and its related side effects? (Select two.)

A. Risk Tracer
B. Terminate Processes Automatically
C. Early Launch Anti-Malware Driver
D. Stop Service Automatically
E. Stop and Reload AutoProtect

Correct Answer: BD

QUESTION 65
An administrator configures the scan duration for a scheduled scan fails to complete in the specified time period. When will the next schedule scan occur on the computer?

A. when the computer reboots
B. when the user restarts the scan
C. at the next scheduled scan period
D. within the next hour

Correct Answer: C

QUESTION 66
A Symantec Endpoint Protection (SEP) administrator receives multiple reports that machines are experiencing performance issues. The administrator discovers that the reports happen about the same time as the scheduled LiveUpdate. Which setting should the SEP administrator configure to minimize I/O when LiveUpdate occurs?

A. Change the LiveUpdate schedule
B. Change the Administrator-defined scan schedule
C. Disable Allow user-defined scans to run when the scan author is logged off
D. Disable Run an Active Scan when new definitions arrive

Correct Answer: D

QUESTION 67
An administrator needs to increase the access speed for client files that are stored on a file server. Which configuration should the administrator review to address the read speed from the server?

A. enable Network Cache in the client's Virus and Spyware Protection policy
B. add the applicable server to a trusted host group
C. create a Firewall allow rule for the server's IP address
D. enable download randomization in the client group's communication settings

Correct Answer: A

QUESTION 68
An administrator changes the Virus and Spyware Protection policy for a specific group that disables Auto-Protect. The administrator assigns the policy and the client systems applies the corresponding policy serial number. Upon visual inspection of a physical client system, the policy serial number is correct. However, Auto- Protect is still enabled on the client system. Which action should the administrator take to ensure that the desired setting is in place on the client?

A. restart the client system
B. run a command on the computer to Update Content
C. enable the padlock next to the setting in the policy
D. withdraw the Virus and Spyware Protection policy

Correct Answer: C

QUESTION 69
Which two settings does an administrator enable to use the Risk Tracer feature in the Virus and Spyware Protection policy? (Select two.)

A. Application and Device Control Policy
B. Tamper Protection
C. Firewall Policy
D. IPS active response
E. Application Learning

Correct Answer: CD

QUESTION 70

What are two criteria that Symantec Insight uses to evaluate binary executables? (Select two.)

A. sensitivity
B. prevalence
C. confidentiality
D. content
E. age

Correct Answer: BE

QUESTION 71
How are Insight results stored?

A. encrypted on the Symantec Endpoint Protection Manager
B. unencrypted on the Symantec Endpoint Protection Manager
C. encrypted on the Symantec Endpoint Protection client
D. unencrypted on the Symantec Endpoint Protection client

Correct Answer: C

QUESTION 72
Which two options are available when configuring DNS change detected for SONAR? (Select two.)

A. Block
B. Active Response
C. Quarantine
D. Log
E. Trace

Correct Answer: AD

QUESTION 73
What does SONAR use to reduce false positives?

A. Virus and Spyware definitions
B. File Fingerprint list
C. Symantec Insight
D. Extended File Attributes (EFA) table

Correct Answer: C

QUESTION 74
Which action does SONAR take before convicting a process?

A. quarantines the process
B. blocks suspicious behavior
C. reboots the system
D. checks the reputation of the process

Correct Answer: D

QUESTION 75
An administrator notices that some entries list that the Risk was partially removed. The administrator needs to determine whether additional steps are necessary to remediate the threat. Where in the Symantec Endpoint Protection Manager console can the administrator find additional information on the risk?

A. Risk log

B. Computer Status report
C. Notifications
D. Infected and At Risk Computers report

Correct Answer: A

QUESTION 76
Which two instances could cause Symantec Endpoint Protection to be unable to remediate a file? (Select two.)

A. Another scan is in progress.
B. The detected file is in use.
C. There are insufficient file permissions.
D. The file is marked for deletion by Windows on reboot.
E. The file has good reputation.

Correct Answer: BC

QUESTION 77
An administrator selects the Backup files before attempting to repair the Remediations option in the Auto-Protect policies. Which two actions occur when a virus is detected? (Select two.)

A. replace the file with a place holder
B. check the reputation
C. store in Quarantine folder
D. send the file to Symantec Insight
E. encrypt the file

Correct Answer: CE

QUESTION 78
In the virus and Spyware Protection policy, an administrator sets the First action to Clean risk and sets If first action fails to Delete risk. Which two factors should the administrator consider? (Select two.)

A. The deleted file may still be in the Recycle Bin.
B. IT Analytics may keep a copy of the file for investigation.
C. False positives may delete legitimate files.
D. Insight may back up the file before sending it to Symantec.
E. A copy of the threat may still be in the quarantine.

Correct Answer: CE

QUESTION 79
A company allows users to create firewall rules. During the course of business, users are accidentally adding rules that block a custom internal application. Which steps should the Symantec Endpoint Protection administrator take to prevent users from blocking the custom application?

A. create an Allow Firewall rule for the application and place it at the bottom of the firewall rules below the blue line
B. create an Allow Firewall rule for the application and place it at the bottom of the firewall rules above the blue line
C. create an Allow All Firewall rule for the fingerprint of the file and place it at the bottom of the firewall rules above the blue line
D. create an Allow for the network adapter type used by the application and place it at the top of the firewall rules below the blue line

Correct Answer: B

QUESTION 80
A company has an application that requires network traffic in both directions to multiple systems at a specific external domain. A firewall rule was created to allow traffic to and from the external domain, but the rule is blocking incoming traffic. What should an administrator enable in the firewall policy to allow this traffic?

A. TCP resequencing
B. Smart DHCP
C. Reverse DNS Lookup
D. Smart WINS

Correct Answer: C

QUESTION 81
A Symantec Endpoint Protection administrator must block traffic from an attacking computer for a specific time period. Where should the administrator adjust the time to block the attacking computer?

A. in the firewall policy, under Protection and Stealth
B. in the firewall policy, under Built in Rules
C. in the group policy, under External Communication Settings
D. in the group policy, under Communication Settings

Correct Answer: A

QUESTION 82
A user is unknowingly about to connect to a malicious website and download a known threat within a .rar file. All Symantec Endpoint Protection technologies are installed on the client's system. In which feature set order must the threat pass through to successfully infect the system?

A. Download Insight, Firewall, IPS
B. Firewall, IPS, Download Insight
C. IPS, Firewall, Download Insight
D. Download Insight, IPS, Firewall

Correct Answer: B

QUESTION 83
A Symantec Endpoint Protection (SEP) administrator creates a firewall policy to block FTP traffic and assigns the policy to all of the SEP clients. The network monitoring team informs the administrator that a client system is making an FTP connection to a server. While investigating the problem from the SEP client GUI, the administrator notices that there are zero entries pertaining to FTP traffic in the SEP Traffic log or Packet log. While viewing the Network Activity dialog, there is zero inbound/outbound traffic for the FTP process. What is the most likely reason?

A. The block rule is below the blue line.
B. The server has an IPS exception for that traffic.
C. Peer-to-peer authentication is allowing the traffic.
D. The server is in the IPS policy excluded hosts list.

Correct Answer: D

QUESTION 84
Which action must a Symantec Endpoint Protection administrator take before creating custom Intrusion Prevention signatures?

A. change the custom signature order
B. create a Custom Intrusion Prevention Signature library
C. define signature variables

D. enable signature logging

Correct Answer: B

QUESTION 85
A Symantec Endpoint Protection administrator needs to prevent users from modifying files in a specific program folder that is on all client machines. What does the administrator need to configure?

A. a file and folder exception in the Exception policy
B. an application rule set in the Application and Device Control policy
C. a file fingerprint list and System Lockdown
D. the Tamper Protection settings for the client folder

Correct Answer: B

QUESTION 86
An administrator tests a new Application and Device Control policy. One of the rule sets being tested blocks the notepad.exe application from running. After pushing the policy to a test client, the administrator finds that notepad.exe is still able to run. The administrator verifies that the rule set is enabled in the Application and Device Control policy. Which two reasons may be preventing the policy from performing the application blocking? (Select two.)

A. The System Lockdown policy includes notepad.exe in the whitelist.
B. System Lockdown has been removed from the client.
C. The Client User Interface Control is set to Client control.
D. The rule set is in Production mode.
E. A rule set with conflicting rules exists higher up in the policy.

Correct Answer: AE

QUESTION 87
A Symantec Endpoint Protection administrator is using System Lockdown in blacklist mode with a file fingerprint list. When testing a client, the administrator notices that at least one of the files on the list is allowed to execute. What is the likely cause of the problem?

A. The application has been upgraded.
B. The Application and Device Control policy is in test mode.
C. A file exception has been added to the Exceptions policy.
D. The Application and Device Control policy is allowing the file to execute.

Correct Answer: A

QUESTION 88
Which step is unnecessary when an administrator creates an application rule set?

A. define a provider
B. select a process to apply
C. select a process to exclude
D. define rule order

Correct Answer: A

QUESTION 89
An administrator needs to learn the applications running on a computer. Which step should the administrator take to configure functionality?

A. configure a local Symantec Endpoint Protection Manager administrator to have rights to view reports only

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

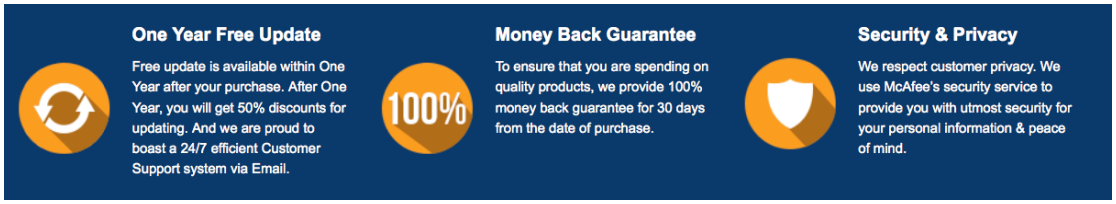
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions