Symantec Messaging Gateway 10.0. Technical Assessment

Number: ST0-199
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Exam A

QUESTION 1
What is the recommended minimum hard-drive size for a virtual instance of Symantec Messaging Gateway 10.0?

A. 80 GB
B. 90 GB
C. 160 GB
D. 180 GB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
What is the recommended minimum hard-drive size for a virtual instance of Symantec Messaging Gateway 10.0?

A. 80 GB
B. 90 GB
C. 160 GB
D. 180 GB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
What are two installation options for Symantec Messaging Gateway 10.0? (Select two.)

A. upgrade from Symantec Brightmail Gateway 8.0.3
B. enable autoupdate in LiveUpdate settings
C. upgrade from Symantec Mail Security for SMTP (SMS-SMTP) 8.0.3
D. OSRestore using the downloadable VMWare OVF template
E. OSRestore from the Symantec Brightmail Gateway 10.0 CD

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Message throughput of a Symantec Messaging Gateway scanner-only appliance can be reduced by which two features? (Select two.)

A. rapid release definitions
B. real-time updates
C. DKIM signing
D. SMTP authentication
E. hourly quarantine expunging

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Symantec Messaging Gateway 10.0 is certified for non-virtual deployment on which hardware devices?

A. Symantec 2950 series appliances
B. Symantec 3570 series appliances
C. Symantec 7100 series appliances
D. Symantec 8300 series appliances

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which two are functions of a Symantec Messaging Gateway 10.0 scanner? (Select two.)

A. provides quarantine storage for messages
B. downloads virus definitions
C. hosts a web server
D. filters the message stream
E. runs expunger agents for the quarantine

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
What is the maximum number of incident folders that may be created in Symantec Messaging Gateway 10.0?

A. 100
B. 1,000

C. 10,000
D. unlimited

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which Symantec Messaging Gateway 10.0 feature is used to organize, monitor, and manage incidents?

A. Regulatory Archives
B. End User Quarantine
C. Regulatory Protocols
D. Content Incident Folders

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
What do content incident folders allow administrators to configure?

A. granular access control
B. the X- header added for client processing
C. the incident folder names passed to the client
D. additional folders where end-users can store junk mail

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which two policy actions are available within Symantec Messaging Gateway version 10.0? (Select two.)

A. create a quarantine incident
B. deliver the message to the Outlook spam folder
C. send notification to the administrator
D. terminate the sender's connection
E. create an informational incident

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
There is a firewall in place between Symantec Messaging Gateway 10.0 and the Internet at the customer site. An administrator needs to use an external NTP server on the Internet for time synchronization. Which port must be open on the firewall to allow this?

A. 22
B. 389
C. 80
D. 123

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What is a valid configuration option for Symantec Messaging Gateway 10.0?

A. one Control Center, one combination control center/scanner
B. one Control Center, three scanners, and one Report Center
C. one combination control center/scanner, and 3 scanners
D. two scanners and one LiveUpdate server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
What is required before completing the bootstrap process of the Symantec Messaging Gateway 10.0 appliance?

A. 30-day temporary license file
B. DNS server IP address
C. SSH access to the appliance
D. MX record created for appliance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

If recipient validation is configured properly, which SMTP response level is given to messages that fail recipient validation queries at connect time?

A. 3xx - Service unavailable
B. 4xx - Temporary delivery failure
C. 5xx - Permanent delivery failure
D. 6xx - Rejected validation failure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which feature places a sender's IP address in a penalty box for sending messages to multiple invalid email addresses?

A. Local Bad Sender IPs
B. Directory Harvest Attack
C. Bounce Attack Detection
D. Connection Classification

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which two tasks can an end-user perform while logged in to the Control Center when authentication and address resolution are enabled? (Select two.)

A. configure personal suspect spam scoring
B. configure personal Good and Bad Sender lists
C. configure personal language preferences
D. configure personal content filtering policies
E. configure personal email digest preferences

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
An organization has an extremely large LDAP database. What is done in Symantec Messaging Gateway 10.0 that will help prevent mail from backing up in the system during the initial directory building process?

A. reduce the length of time that logs and quarantine items are kept in the database
B. configure the control center to download the complete directory of users each night
C. the appliance fails open during the initial phase of deployment to prevent email from backing up during the initial directory building process
D. preload the directory data cache

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which two functions of Symantec Messaging Gateway 10.0 can use information retrieved from a directory data source? (Select two.)

A. masquerading
B. routing
C. annotation
D. reputation
E. authentication

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
When configuring remote logging, where are the logs redirected?

A. the primary control center
B. Symantec System Incident Manager (SSIM)
C. Application Eventlog
D. syslog

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which log would an administrator access to determine why an email was deleted by the scanner?

A. Update.log
B. Message Audit logs
C. Admin Audit logs

D. Messaginglog.log

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which logs will help an administrator determine why antispam rules have failed to update?

A. Antispam Update logs
B. LiveUpdate logs
C. Conduit logs
D. Appliance syslog

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Having received a targeted attack from a spoofed email domain, a company wants to take advantage of DKIM validation for inbound mail. The messaging administrator has enabled sender authentication and DKIM validation and now needs to configure a content filtering policy to quarantine any messages that fail. Which condition should be met for the content filtering policy to fire?

A. The envelope sender email address contains "dkim=fail".
B. The message header contains "dkim=fail".
C. The file metadata MIME type is "dkim=fail".
D. The text in the subject, body, or attachments contains "dkim=fail".

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
How does enabling and configuring sender authentication options in Symantec Messaging Gateway 10.0 help to protect against spam?

A. by protecting against messages sent from trusted partners
B. by protecting against messages sent using a Sendmail MTA
C. by protecting against messages with a forged message ID
D. by protecting against messages with forged sender domains

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
What is an advantage of Symantec Content Encryption over TLS encryption?

A. ensures compliance with government-mandated regulations
B. TLS encryption provides better security than content encryption.
C. may be implemented without requiring SSL certificates for each scanner
D. ensures secure end-to-end delivery of sensitive messages

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Symantec Messaging Gateway 10.0 includes a policy-based encryption feature. How is this new feature licensed?

A. The license is included with Symantec Protection Suite.
B. The license is included with Symantec Messaging Gateway 10.0.
C. The license is included with Symantec Content Encryption.
D. The license is available with a PGP Universal license.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which command allows the administrator to track messages from the command line interface (CLI)?

A. track message
B. monitor
C. malquery
D. message query

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

Which command is used to collect the configuration and log files from the command line interface (CLI)?

A. diagnostics
B. mallog
C. collect-logs
D. cc-config

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
An administrator needs to determine which policies have triggered for a particular message. Which troubleshooting tool will help to identify issues with policy precedence and actions?

A. Incident Match log
B. Filtering Policy report
C. Filtering Precedence Exception report
D. Message Audit log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
An administrator recently investigated the debug logs for Symantec Messaging Gateway 10.0 and resolved an issue. A few days later the administrator discovers that the disk storage is filling up quickly. What is the likely cause?

A. logging severity is set to All
B. local log level is set to Debug
C. logging severity is set to Informational
D. remote syslog server is down

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
An employee reports that a message sent to a customer was never received by the customer. The employee provides sufficient information for the administrator to find the message using the Message Audit log. The employee wants to know where that

message has gone. Which section of the Message Audit log detail page will provide this information?

A. message data
B. actions taken
C. intended recipients
D. authenticated username

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Where does an administrator specify how often a report is run?

A. Reports -> Schedule
B. Reports -> Create a Reports
C. Reports -> Favorite Reports
D. Reports -> Schedule Reports

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which additional Email Reports Data collection must be enabled to track Top Probe Accounts via reports?

A. Spam and Unwanted Mail
B. Submissions
C. Sender IP connections
D. Invalid Recipients

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which two report file formats are available in Symantec Messaging Gateway 10.0 for executive summary reports? (Select two.)

A. CSV
B. PDF

C. DOCX
D. XML
E. HTML

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which two features of Symantec Messaging Gateway 10.0 can be implemented to address the need of Data Loss Prevention (DLP)? (Select two.)

A. setup content filtering rules using pre-defined content category dictionaries
B. setup connection to any industry standard DLP product
C. setup content filtering rules to strip out any executable content
D. enforce antivirus scanning for all outbound email
E. setup connection to Symantec's DLP Enforce product

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
On which two servers can the administrator remediate Data Loss Prevention (DLP) incidents? (Select two.)

A. The destination mail server, such as Microsoft Exchange or Lotus Domino.
B. The Symantec Messaging Gateway Scanner.
C. The Symantec Messaging Gateway Control Center.
D. The Symantec DLP Network Prevent server.
E. The Symantec DLP Enforce server.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
The administrator of a Japanese organization wants to view dates and times within the web-based interface of Symantec Messaging Gateway 10.0 in Japanese format. Which step during the site setup wizard allows the administrator to meet this requirement?

A. System Locale Setup
B. Language Setup
C. Country Setup
D. Time Zone Setup

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which networking parameter can be configured during site setup wizard?

A. MTU size
B. DNS server
C. default gateway
D. virtual IP address

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
After the bootstrap process is completed, which action is unavailable through the web- based interface?

A. selecting the time zone
B. defining the Messaging Gateway role
C. changing the administrator's password
D. defining the IP address of the DNS server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which two should be verified in the Message Audit log when testing a message against a newly created compliance policy? (Select two.)

A. message queue ID
B. verdict
C. actions taken
D. policy name
E. message ID

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which two can be used to verify that Symantec Messaging Gateway 10.0 is processing messages? (Select two,)

A. view the Message Audit log
B. view the Fastpass log
C. view message headers
D. view the invalid recipients header
E. view the Admin Audit log

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
In addition to a configured seed, which other characteristic does Symantec Messaging Gateway 10.0 use to create a unique tag for Bounce Attack Prevention?

A. message ID
B. IP address
C. fully qualified hostname
D. date

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
A Symantec Messaging Gateway 10.0 administrator is creating a new spam policy and needs to choose a message condition. Which two are valid message conditions? (Select two.)

A. a message that contains a header from DLP
B. a message that is spam or suspected spam
C. a message that contains prepended notation
D. a message that is unscannable
E. a message that fails bounce attack validation

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Probe accounts should be created from which source of email addresses?

A. automatically generated using the built-in tool
B. addresses of previous employees
C. current NDR reports

D. invalid recipient lists

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A Symantec Messaging Gateway 10.0 administrator needs to prevent bounce attacks. Where should the administrator enable this feature?

A. Bad Senders policy
B. Antivirus policy
C. Directory Harvest Attack policy
D. Antispam policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
After a configurable period of time, a suspect virus is released from the Suspect Virus Quarantine. What happens to it next?

A. An alert is sent to the email administrator.
B. The attachment is removed and the original message is delivered to the recipient.
C. It is rescanned.
D. It is moved to quarantine.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which listener accepts messages from the Brightmail Engine for carrying out actions based on the rendered verdicts?

A. Inbound
B. Conduit
C. MTE

D. MTA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which URL must be accessed to successfully register a newly added Symantec Messaging Gateway 10.0 license file?

A. aztec.brightmail.com
B. license.symantec.com
C. register.brightmail.com
D. register.symantec.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which MTA operation is used if queues need to be drained to remove a host from use and continue scanning and delivery of messages?

A. delete the Scanner from the Control Center so that it is no longer used
B. set the Scanner configuration to "Pause message scanning and delivery"
C. set the Scanner configuration to "Do not accept incoming messages"
D. disable the Conduit so that new messages are not accepted

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
During which phase of inbound message flow does Symantec Messaging Gateway 10.0 accept, reject, or defer messages on the basis of the message envelope?

A. SMTP delivery
B. SMTP firewall
C. SMTP session
D. Connection Classification

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which two options are valid for pre-configured actions for the language identification feature in Symantec Messaging Gateway 10.0? (Select two.)

A. hold message received in the following languages in the Suspect Spam Quarantine
B. do not receive mail in the following languages
C. send notification to the recipient for messages rceived in the following languages.
D. only receive mail in the following languages
E. add an X-Bulk header to messages received in the following languages

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which two actions must be taken to allow end-users to create personal Good and Bad Senders lists? (Select two.)

A. add "Hold message in Spam Quarantine" action to Local Bad Senders domains
B. check the option "Enable end-user settings for this policy group"
C. configure an LDAP source with Authentication and Recipient Validation functions
D. configure an LDAP source with Authentication and Routing functions
E. configure an LDAP source with Authentication and Address Resolution functions

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
What happens to a message after it has been identified as a suspect virus and placed into the suspect virus quarantine?

A. It is automatically deleted after 7 days.
B. It is rescanned when the configured hold time has elapsed.
C. It is stored in the Central Quarantine Server.
D. It is forwarded to Symantec Security Response.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53

Which Symantec Messaging Gateway 10.0 feature will change the original domain of an internal user relaying mail outside of an organization?

A. address masquerading
B. address aliasing

C. domain mapping
D. content filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
A customer receives large amounts of non-spam mail from thousands of different users, which consumes significant resources on Symantec Messaging Gateway 10.0. Which feature should be enabled to improve system performance while minimizing the risk of false positives?

A. Creation of custom spam rules using SenderID
B. Fastpass
C. Domain whitelisting
D. Sender authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
An administrator needs to determine whether a sending MTA is being throttled by Symantec Messaging Gateway 10.0. Where is this information located?

A. Reputation Summary report
B. IP reputation lookup table
C. SMTP server logs
D. message audit logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
An organization wants to be extremely aggressive in identifying new and emerging virus threats. Which action should be recommended?

A. enable the use of rapid release definitions
B. enable zero-day virus protection
C. set the virus policy to automatically delete viruses
D. set LiveUpdate to check for definitions every five minutes

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
True file typing is a feature used to combat which behavior?

A. intentionally malforming the MIME headers in order to bypass virus scanning of attachments
B. removing or disguising extensions to bypass virus scanning
C. obfuscating a directory harvest attack
D. tricking users into launching executable files

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Outgoing messages need to be checked for specific words and phrases. Any messages containing the listed words should be held for review. Which content filtering resource is used for this requirement?

A. Directories
B. Dictionaries
C. Notifications
D. Annotations

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
An administrator works for a pharmaceutical company that distributes Drug X. A content filtering policy using the premium compliance "Prescription Drug Names" dictionary resource (which includes Drug X as a predefined phrase), blocks any email from the Marketing department containing the drug name. Marketing has indicated that this is unacceptable but wishes to continue to block the use of other words or phrases in that dictionary. How can the administrator adjust the resources used by the current content filtering policy to resolve the Marketing department issue?

A. disable Drug X from the "Prescription Drug Names" dictionary
B. add Drug X to the "Prescription Drug Names" dictionary
C. enable Drug X in the "Prescription Drug Names" dictionary
D. delete Drug X from the "Prescription Drug Names" dictionary

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which two actions are valid for a content compliance policy? (Select two.)

A. edit the message to delete the offensive content
B. add a header to the message
C. drop the connection to the offending mail server
D. forward the message
E. flag the message for further scanning

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
The helpdesk consistently receives calls from end-users asking why some attachments are stripped from their outbound email messages. How can the messaging administrator configure the content policy to inform the sender when and why this occurs?

A. add a notification action to the content filtering policy
B. enable message quarantine for outbound policy violations
C. add an action to create an end-user incident
D. add an action to modify the subject line

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
How are content filtering policies different from spam and virus policies?

A. Content filtering policies use system-defined verdicts.
B. Spam and virus polices use administrator-defined verdicts.

C. Spam and virus policies use system-defined verdicts.
D. Content filtering policies use end user-defined verdicts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
What must be done before using Spam Quarantine?

A. configure address resolution
B. configure groups to have a policy to quarantine messages
C. configure a partition for use by Spam Quarantine
D. configure Spam Scan settings to identify suspected spam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
A message released from Spam Quarantine is delivered to the intended recipient. Under the default configuration, where is a copy of the misidentified message also sent?

A. abuse@brightmail.com
B. Symantec Security Response
C. the email address configured as the administrator for the control center
D. Symantec's Global Intelligence Network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
What two actions can allowed end-users do to submit samples to Symantec and have custom anti- spam rules created? (Select two.)

A. submit a sample to Symantec using the Email Submission Client
B. flag messages in their web-based SMG quarantine page as being spam and submitting the results
C. forward spam samples to abuse@symantec.com with a subject of "MISSED SPAM"
D. move the message into the included "Junk E-mail" folder available in Outlook
E. submit a sample to Symantec using the Email Submission Client available for Lotus Domino

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
What are two benefits of customer-specific spam rules? (Select two.)

A. provides a wizard style tool enabling administrators to create rules against spam
B. provides a mechanism to quickly block local or targeted attacks
C. enables the administrator to report spammers to Symantec Global Intelligence Network
D. adds the IP of selected spammers to the lowest bucket in the Connection Throttling module
E. provide fast protection against messages Symantec may not define as spam

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
When should Connection Classification be enabled?

A. when Fastpass access is needed to log the connection
B. when deployed at the edge of the network
C. when another gateway handles the messages first
D. when handling mail for multiple internal domains

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
When should Connection Classification be enabled?

A. when Fastpass access is needed to log the connection
B. when deployed at the edge of the network
C. when another gateway handles the messages first
D. when handling mail for multiple internal domains

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
What happens to an IP listed in the Fastpass exclusions?

A. The IP will not be processed for spam, but will still be scanned for malware.
B. The IP will be excluded from spam scanning.
C. The IP will never get a Fastpass.
D. The IP will be excluded from compliance scanning.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
When enabling Connection Classification, how many messages must be processed in learning mode before messages can be deferred?

A. 5,000
B. 10,000
C. 20,000
D. 50,000

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A diagnostics package for a scanner-only appliance can be generated from the GUI in Symantec Messaging Gateway 10.0. If the package is small (less than 5 MB), which transfer protocol type should be used by the administrator to verify the diagnostics package before providing it to technical support for analysis?

A. SMTP
B. download to desktop
C. FTP
D. SCP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
What should an administrator do before performing a software update of Symantec Messaging Gateway 10.0?

A. store backup on local server
B. store backup on a remote location using FTP
C. encrypt local backup
D. purge all backups from the appliance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which command line interface (CLI) command displays the update.log to check the progress of a software update of Symantec Messaging Gateway 10.0?

A. tail
B. watchlog
C. update.pl
D. version -l

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Before performing a software update on a scanner-only appliance, which MTA operation/mode should be chosen if there are messages in the queues?

A. pause the MTA
B. flush all delivery queues
C. pause message scanning and delivery
D. do not accept incoming messages

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
How could an administrator improve Control Center performance of Symantec Messaging Gateway 10.0?

A. increase the log rotation frequency
B. increase the number of service threads
C. reduce the amount of reporting data
D. restrict user access to the spam quarantine

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
An employee reports that a message sent to a customer was rejected. The employee provides sufficient information for the administrator to find the message using the Message Audit log. The employee wants to know why that message was blocked. Which section of the Message Audit Log detail page would provide this information?

A. Verdict(s)
B. Action(s)
C. IP Blocklist Lookup Tool
D. Block Reason

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Symantec Messaging Gateway 10.0 is running out of disk space due to storing extended logs. The administrator is required to store extended log data for more than a year. Which action should the administrator take?

A. lower the maximum log storage limit
B. deploy Control Center on virtual appliance and add more disk space
C. configure remote logging
D. add higher capacity disks to appliace RAID array

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
After configuring the directory data source, which tab must be selected to configure Invalid Recipients functionality?

A. Administration tab
B. Protocols tab
C. Reputation tab
D. DHA tab

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
By default, which port does Symantec Messaging Gateway 10.0 use to retrieve updated spam definitions?

A. 389
B. 443
C. 8080
D. 41002

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
What will trigger a spam policy by default in Symantec Messaging Gateway 10.0?

A. adding a text file attachment with the word SPAM to the message
B. inserting the header X-Bulk: into the message header
C. prepending the subject line of the message with the following: [SPAM TEST]
D. inserting the header X-Advertisement: spam into the message header

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which feature, when enabled through the directory data sources, allows third party MTAs the ability to relay through Symantec Messaging Gateway 10.0 and protects it against becoming an open relay?

A. MTA verification
B. Recipient address validation
C. TLS certificate authentication
D. SMTP authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82

Which Symantec Messaging Gateway 10.0 feature improves responsiveness to new spam threats and increases overall antispam effectiveness?

A. rapid release definitions
B. Fastpass
C. microupdates
D. real time updates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
An organization is receiving spam because of small targeted attacks from unknown senders. Which Symantec Messaging Gateway 10.0 feature should help slow down these types of attacks?

A. Global Bad Senders list
B. directory harvest attack prevention
C. Global reputation analysis
D. Connection classification

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
What is the source of information used to populate the Global Good and Global Bad senders list?

A. Multiple DNS-based IP reputation services
B. Proprietary feed from MessageLabs
C. Reputation data from the Symantec Global Intelligence Network
D. Global reputation data from Symantec Protection Center

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Symantec Messaging Gateway 10.0 will be deployed to receive mail directly from the Internet. In this situation, which option should be selected within the Inbound Mail Filtering - Accepted Hosts step of the site setup wizard?

A. enable MX lookup
B. define a list of domains
C. specify IP addresses/domains
D. select all IP addresses

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
The Symantec Messaging Gateway 10.0 appliance will be deployed with the following topology: Internet Default Gateway (10.10.10.1) <--> Email Gateway (10.10.10.11) <- -> Symantec Messaging Gateway (10.10.10.21) <--> Internal Mail Server (10.10.10.31) Which IP address should be specified in the Mail Filtering - Non-local Mail Delivery page of the site setup wizard?

A. 10.10.10.1
B. 10.10.10.11
C. 10.10.10.21
D. 10.10.10.31

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
During the installation and configuration process, when will Symantec Messaging Gateway 10.0 require access to the network?

A. prior to the bootstrap process
B. when defining the DNS server
C. when defining the Gateway address
D. prior to accessing the site setup wizard

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
What is required before attempting installation of the Symantec Messaging Gateway 10.0 appliance?

A. console access to the appliance

B. DVD-ROM drive listed on hardware compatibility list
C. valid license file
D. machine account created in Active Directory

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which TCP port is used for communication between the Control Center and the scanner(s)?

A. 41001
B. 41002
C. 41004
D. 41080

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Where are options for backup and restore of Symantec Messaging Gateway 10.0 located?

A. Administration -> Version
B. Administration -> Utilities
C. Administration -> Restore/Download
D. Administration -> Updates

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Following the leak of confidential business contracts, a company's Legal department mandates that all outbound communication from the Finance department must be secure at all times. Which two policy strategies can help the messaging administrator accomplish this in Symantec Messaging Gateway 10.0? (Select two.)

A. deliver message using TLS
B. block direct client access to corporate email servers
C. deliver message with notification
D. deliver message with content encryption

E. configure firewall to only accept outbound SMTP connections from the Symantec Messaging Gateway scanners

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
What are two benefits of using attachment list policy resources in Symantec Messaging Gateway 10.0? (Select two.)

A. can help prevent confidential information from leaving the company
B. can provide another level of defense against malware
C. can increase message processing speed
D. can protect against drive-by downloads
E. can help prevent directory harvest attack (DHA)

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
In which two situations are multiple group policies useful? (Select two.)

A. when the entire organization wants to delete spam
B. when only the Human Resources department wants to receive spam
C. when only the Engineering department wants to keep message logs
D. when only the Legal department should be allowed to send archive files
E. when all of the departments want to scan outbound messages

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Legitimate email from xCorp is being rejected by Symantec Messaging Gateway 10.0 at ZZ Inc. How can a ZZ Inc. email administrator troubleshoot this issue?

A. Add the xCorp MTA IP address to the Fastpass table.
B. Add the xCorp MTA IP address to the Global Good Senders list.
C. View the reputation of the xCorp MTA using the Spamhaus IP Address Lookup Tool.
D. View the reputation status of the xCorp MTA IP address via the IP Reputation lookup tool.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
What is the default action taken during an email virus attack?

A. delete the message
B. throttle the network connection
C. reject SMTP connection
D. defer SMTP connection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
With Fastpass enabled, which two verdicts may be excluded for messages with a pass? (Select two.)

A. Spam
B. Suspected Spam
C. Virus
D. Suspected Virus
E. Compliance

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
What can administrators do in order to receive custom anti-spam rulesets?

A. forward spam samples to abuse@brightmail.com
B. log a support case and submit samples to Symantec for analysis
C. create a content filter rule to block the message based on the spam sample
D. enable the customer-specific rules feature and submit unwanted messages

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which two statistics can the administrator view regarding the custom anti-spam rulesets? (Select two.)

A. the "top-submitters" of missed spam or false positive detections
B. the "top submitters" of messages that are not valid and did not generate a custom rule
C. how many emails have been submitted for custom antispam rules
D. the effectiveness of the custom antispam rulesets compared to Symantec's rulesets
E. the top senders of messages detected by custon antispam rulesets

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A company uses multiple control centers. What must be done to ensure legitimate NDRs are recognized by Bounce Attack Prevention across all scanners?

A. configure the same seed value on each control center
B. configure the same administrator email address across both control centers
C. configure the same seed value on each scanner
D. configure both control centers with the same internal email hosts

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
What is the maximum number of rows a report can have?

A. 100 rows
B. 1,000 rows
C. 10,000 rows
D. 100,000 rows

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
What is the default report data retention period?

A. 7 days
B. 14 days
C. 28 days
D. 90 days

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
An administrator wants to ensure high performance and failover access between the LDAP servers and Symantec Messaging Gateway 10.0. Which configuration mode will help ensure this?

A. configure DNS to accept dynamic updates
B. setup multiple LDAP sources
C. round robin DNS
D. scanner load balancing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Which directory data source function must be enabled to help prevent a directory harvest attack?

A. Active Directory connector
B. Dynamic Data Sourcing
C. LDAP authentication
D. Recipient validation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
An organization would like to participate in the Symantec Probe Network without having to manually create decoy email accounts. The organization wants to make sure that the addresses that participate in the Symantec Probe Network are currently receiving email. Which directory data source function should be enabled to help in this situation?

A. recipient validation

B. address resolution
C. SMTP authentication
D. LDAP routing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
How does Symantec DLP communicate with Symantec Messaging Gateway (SMG) to indicate what type of incident (if any) is related to a given message?

A. Symantec DLP uses the ICAP protocol to indicate if a message is clean, or if it violated any defined policies.
B. Symantec DLP will add information into the message that can be interpreted by SMG and then send it to SMG via SMTP.
C. Symantec DLP will quarantine messages that violate established policies, blocking it from SMG.
D. Symantec DLP will use TLS to send a notification message to the SMG server for any content violations.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
What are two functions of the Control Center? (Select two.)

A. It provides message management services.
B. It downloads spam definitions.
C. It hosts Spam Quarantine.
D. It downloads virus definitions.
E. It runs filters.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
During which phase of outbound message flow does Symantec Messaging Gateway 10.0 determine whether the number of recipients exceeds the good number of recipients per message?

A. message routing
B. message delivery
C. outbound SMTP session
D. outbound SMTP connection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
How should an administrator stop inbound mail using the command line interface (CLI)?

A. use mta-control
B. use mta-stop
C. use mail-control
D. use mail-stop

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
How can an administrator view log data in real time?

A. in the UI select Reports -> view logs
B. from the command line interface (CLI) run the watchlog -l command
C. from the command line interface (CLI) run the tail -f command
D. from the command line interface (CLI) run the monitor -f command

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
What is the function of a sender authentication scheme?

A. to check the IP reputation of a sending MTA at connection time
B. to verify that the sending MTA is authorized to send mail for a given domain
C. to enforce two-factor authentication between sending and receiving MTAs
D. to ensure that senders using content encryption can bypass spam scanning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
When configuring DKIM signing, how should the domain key generated from the public RSA key be published?

A. as a text record in the DNS zone for the sending domain
B. in plain text as part of the SMTP outbound greeting
C. as a .txt file on the Internet facing the Symantec Messaging Gateway
D. as a .txt file on the sending domain corporate website

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
What is one effect of deploying a Symantec Messaging Gateway scanner between an Internet email gateway and the internal groupware mail server?

A. Symantec Messaging Gateway delivery queues may backup due to the network latency of an extra hop.
B. Symantec Messaging Gateway scanners might identify the IP address of the internal gateway MTA as a source of spam.
C. Symantec Messaging Gateway scanners will not be able to provide antispam services.
D. Symantec Messaging Gateway scanners will grant the internal gateway MTA a Fastpass.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Which prerequisite must be met to take advantage of the Connection Classification and Fastpass features?

A. Symantec Messaging Gateway must use a virtual IP address.
B. Symantec Messaging Gateway must be configured with two network interfaces.
C. Symantec Messaging Gateway must be the first SMTP hop into the network.
D. Symantec Messaging Gateway must be configured in scanner-only mode.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
What is the current name of the LDAP synchronization technology used within the Symantec Messaging Gateway?

A. Dynamic Data Cache
B. Directory Data Service
C. Active Directory
D. Domain Controller Interface (DCInterface)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Which Directory Data Source function must be configured to enable end-user spam quarantine?

A. SMTP authentication
B. address resolution
C. recipient validation
D. authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
What is the integrated encryption action within Symantec Messaging Gateway 10.0?

A. deliver messages with S/MIME encryption
B. deliver messages with content encryption
C. deliver messages using TLS

D. deliver messages with PGP encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
What is the default time period that a suspect virus can reside in the Suspect Virus Quarantine?

A. 6 hours
B. 12 hours
C. 24 hours
D. 48 hours

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Bounce attack prevention is enabled. An incoming non-delivery report (NDR) is received and its signature fails to be verified. What does Symantec Messaging Gateway 10.0 do with the message by default?

A. forwards it to the administrator
B. rejects the message
C. forwards it to suspect spam
D. sends it to Symantec Security Response

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
An administrator tests the default antivirus policies by sending a message with an encrypted attachment. When the administrator checks the recipient inbox, what appears?

A. The test email appears with a modified subject line.
B. A system-generated message appears concerning an unscannable attachment.
C. A message with a pointer to the Suspect Virus Quarantine appears.
D. The email is missing due to deletion by the system.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
How could an administrator filter email more aggressively by adjusting the suspected spam score?

A. Raise the suspected spam score from the default to 99.

B. Lower the suspected spam score from the default to 60.
C. Lower the suspected spam score from the default to 75.
D. Raise the suspected spam score from the default to 72.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
Which type of information can be found on the Status dashboard of Symantec Messaging Gateway 10.0?

A. System uptime, licenses installed, and software version
B. Inbound SMTP Authorization Summary
C. Top Content Filter Sender Summary
D. Inbound Email Message Summary

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: