250-556.VCEplus.premium.exam.70q

Number: 250-556
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

250-556

Administration of Symantec ProxySG 6.7

Version 1.0

Exam A

QUESTION 1

When will a policy trace report a rule processing result of “N/A”? (Choose the best answer.)

A. When the layer containing the rule is disabled
B. When the rule is not reached during evaluation
C. When the rule makes no sense for the specific transaction being processed
D. When the rule is contradicted by a subsequent rule

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2 What is a component of a proxy service listener? (Choose the best answer.)

A. Encryption hash
B. Source IP address
C. Proxy mode
D. Proxy type

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 Which service is provided by the ProxySG? (Choose the best answer.)

A. Virus scanning
B. Strong authentication
C. Edge routing
D. Sandboxing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4 Which best describes BCAAA? (Choose the best answer.)

A. An intermediary between the ProxySG and an authentication server
B. An application that sends sysinfo snapshots to Symantec support
C. Symantec’s internal authorization and authentication service
D. A utility that allows a direct connection between the ProxySG and an authentication domain.

Correct Answer: A
Section: (none)

Explanation
Explanation/Reference:

QUESTION 5 Which two (2) categories of traffic are typically left encrypted?
(Choose two.)

A. Gambling
B. News Media
C. Social Media
D. Financial Services
E. Health

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
When must BCAAA be used? (Choose the best answer.)

A. When an administrator needs to establish more than one Schannel to increase performance.
B. When more than one ProxySG are deployed
C. When the ProxySG is unable to directly utilize APIs that require traditional operating systems.
D. When Basic credentials are used

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 Which type of object is a Notify User object in the VPM? (Choose the best answer.)

A. Destination
B. Action
C. Track
D. Source

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8 Which two (2) situations might require a reverse DNS lookup?
(Choose two.)

A. If the access log is enabled and a field in the access log requires a hostname
B. If both the primary and alternate forward DNS servers go down
C. If primary authentication fails
D. If a policy trigger event requires it

E. If a forward DNS lookup fails
Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 What is the default TCP port for HTTP? (Choose the best answer.)

A. 20
B. 443
C. 80
D. 43

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10 What is typically the biggest load on a CPU when managing encrypted traffic? (Choose the best answer.)

A. Emulating certificates
B. Using the SHA-2 hash function
C. Using RSA encryption
D. The need for redirection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
How does an administrator create a single group in policy that includes multiple client addresses? (Choose the best answer.)

A. Create a combined policy object.
B. Include the addresses in a layer guard.
C. This can only be done using CPL.
D. Use a dedicated layer.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12 In which caching technique does the ProxySG open multiple server connections to retrieve objects referenced on a web page before the client actually issues the requests for those objects? (Choose the best answer.)

A. Popularity contest
B. Cost-based deletion

C. Asynchronous adaptive refresh
D. Pipelining

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 Which service setting determines whether the traffic is passed to the SSL proxy or the HTTP proxy when a browser is configured to use an explicit proxy connection to the ProxySG? (Choose the best answer.)

A. Enable SSL/TLS
B. Detect protocol
C. Authenticate-401
D. Forward client cert

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14 Which two (2) locations is the WebFilter database stored in? (Choose two.)

A. At several data centers around the world
B. In the WebPulse data cache
C. On clients' mobile devices
D. On a properly licensed ProxySG
E. Symantec Management Center

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
What should an administrator utilize in policies to specify which traffic should be decrypted? (Choose the best answer.)

A. Listeners
B. URL categories
C. The SSL Proxy
D. All proxy services

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which log format is associated with the main log facility by default? (Choose the best answer.)

A. http
B. elff
C. main
D. bcreportermain_v1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17 Which two (2) errors are the most common certificate errors? (Choose two.)

A. The server does NOT recognize the ProxySG.
B. The client does NOT trust the server.
C. The client does NOT trust the ProxySG.
D. The ProxySG does NOT trust the server.
E. The server does NOT trust the client.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
How does the ProxySG handle a rule that contains a syntax error when the ProxySG processes installed policy as part of a client transaction? (Choose the best answer.)

A. The ProxySG changes the transaction status to Deny and makes an entry in the event log
B. The ProxySG stops processing of the layer containing the rule and continues with the next layer, if any
C. This is NOT possible; rules with syntax errors are unable to be installed.
D. The ProxySG skips the rule and does NOT change the accept or deny status of the transaction

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19 How can an administrator determine the serial number of the ProxySG in the Management Console? (Choose the best answer.)

A. This information is not visible from the Management Console
B. Go to Statistics > Advanced
C. Go to Configuration > Network
D. The serial number is contained in the top right Management Console banner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 Which kind of authentication credentials might Schannel congestion in IWA direct realms be an issue with? (Choose the best answer.)

A. NTLM
B. Surrogate credentials
C. Kerberos
D. Basic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 Which Symantec product is best suited for simultaneously administering a large number of ProxySG appliances? (Choose the best answer.)

A. PacketShaper
B. Reporter
C. Management Center
D. Content Analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22 How does a network administrator access sysinfo files? (Choose the best answer.)

A. Through the CLI
B. Through the Management Console
C. By creating a sysinfo layer in the VPM
D. Through the use of an advanced URL in a browser

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23 What does it mean if WebPulse returns a URL category of “Pending”? (Choose the best answer.)

A. The URL has NOT been categorized by WebFilter
B. Background categorization is being performed in WebPulse
C. An exception is being sent to the client
D. The ProxySG waits before applying policy to the request

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 24 How does an administrator view policy coverage statistics? (Choose the best answer.)

A. View the Policy Coverage statistics section of the sysinfo.
B. Use an advanced URL.
C. Create a dedicated layer in the VPM.
D. Use a global policy trace.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
In which caching technique are objects that require more server-side bandwidth and response time less likely to be deleted from the cache? (Choose the best answer.)

A. Round robin
B. Cost-based deletion
C. Popularity contest
D. Asynchronous adaptive refresh

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
What must the virtual URL point to, when the ProxySG utilizes a virtual URL for user authentication in a transparent deployment? (Choose the best answer.)

A. The IP address of the origin content server
B. The IP address of the ProxySG
C. A hostname that the user agent can DNS-resolve to an IP address
D. The hostname of the origin content server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27 What are two (2) access methods to the ProxySG? (Choose two.)

A. From a smartphone running the Symantec app
B. Via the enterprise wireless network
C. From the front panel of the appliance
D. A direct connection via a serial cable to the serial console
E. From the back panel of the appliance

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28 Which section of a policy trace would an administrator locate the original HTTP GET request in? (Choose the best answer.)

A. Connection info
B. HTTP section
C. Policy decision
D. Header

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29 What is a Visual Policy Manager (VPM) trigger object? (Choose the best answer.)

A. Action
B. Rule
C. Source
D. Layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30 Which two (2) services are provided by the ProxySG? (Choose two.)

A. Virus scanning
B. Sandboxing
C. Encrypted traffic management
D. Policy enforcement
E. Forensic analysis

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31 What best describes SGOS? (Choose the best answer.)

A. It is Linux-based
B. It is a custom-built operating system
C. It is a Symantec proprietary implementation of Unix
D. It is Windows-based

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 32 Where does the ProxySG get the text of the exception page, when it sends an exception page to a client? (Choose the best answer.)

A. From the VPM-XML file
B. From WebPulse
C. From the exception definition stored on the ProxySG
D. From Symantec Technical Support

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33 Which two (2) files does the VPM update on the ProxySG when policy created in the VPM is installed? (Choose two.)

A. Local policy file
B. Central policy fileC. VPM-CPL file
D. Default policy file
E. VPM-XML file

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34 Which two (2) items are considered external dependencies? (Choose two.)

A. Policy
B. DNS
C. CPU
D. Authentication
E. Memory

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
What is a drawback to utilizing apparent data types to detect the file type? (Choose the best answer.)
A. Does not block “drive-by” malware installation
B. Less accurate than HTTP content type detection
C. Presents a security risk

D. Most resource-intensive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36 How does a server know where to retrieve the requested information when it receives a GET request method? (Choose the best answer.)

A. The server examines the certificate of the requesting IP address
B. The URL is in the GET request
C. The server retrieves it from the server cache
D. The server must return a response message requesting the URL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37 What allows WebPulse to provide real-time revisions to the WebFilter database? (Choose the best answer.)

A. Dynamic categorization
B. Creating a local database
C. Threat risk levels
D. Configuring application controls

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38 Which is responsible for detecting incoming traffic that matches specific IP addresses or subnets? (Choose the best answer.)

A. Listeners
B. Services
C. TCP tunnels
D. Proxies

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 39 What is the primary benefit of using Integrated Windows Authentication (IWA) authentication realms? (Choose the best answer.)

A. Single sign-on experience for users
B. Better performance by using NTLM credentials
C. Ability to use Kerberos credentials

D. Greater security than LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40 Which two (2) methods are able to be used to regain access to the setup console if an administrator loses the password? (Choose two.)

A. Access the ProxySG from another ProxySG
B. Open a serial connection, and use the CLI command restore-defaults factory-defaults
C. Use Management Center to access the setup console
D. Use the front panel buttons and screen, if available on this model, to reset the password
E. Press Control + ALT + DEL

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41 What happens when the ProxySG discovers a match for a rule in policy? (Choose the best answer.)

A. The ProxySG stops further processing in the layer containing the rule.
B. The ProxySG continues processing to see whether a further rule might negate the first rule.
C. It depends on the default policy configured.
D. The ProxySG stops further processing and executes the rule.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42 Which diagnostic tool allows an administrator to examine how the ProxySG has applied policy to a particular request? (Choose the best answer.)

A. Policy/Statistics
B. Policy monitor
C. Policy tracing
D. Packet capture

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 43 Which log facility is used to log HTTP traffic by default? (Choose the best answer.)

A. bcreportermain_v1

B. main
C. http
D. elff

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44 Which section of the sysinfo file would persistent data manager (PDM) information be found within? (Choose the best answer.)

A. Configuration
B. Statistics
C. Logs
D. System states

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45 What are the building blocks of conditions when building policies in CPL? (Choose the best answer.)

A. Triggers
B. Properties
C. Rules
D. Layers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46 Where does ProxySG object caching usually result in the most bandwidth savings? (Choose the best answer.)

A. On the server side
B. On the ProxySG
C. On the client side
D. On the enterprise WAN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47 Under which conditions does a policy-driven trace generate a trace? (Choose the best answer.)

A. Only if a global policy trace is NOT enabled
B. Only if the rule to which it is associated is triggered
C. Only if a global policy trace fails
D. Only if WebPulse is enabled

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48 What are the four principal policy checkpoints in the order they are reached, in a typical client HTTP request? (Choose the best answer.)

A. Client in, server out, server in, client out
B. Client in, server out, client out, server in
C. Client in, server in, client out, server outD. Client in, server in, server out, client out

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49 When can more than one authentication realm be active at any given time on the ProxySG? (Choose the best answer.)

A. Only in explicit mode
B. Never
C. Only in transparent mode
D. When policy is being evaluated

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50 Where can an administrator create a new built-in exception on the ProxySG? (Choose the best answer.)

A. An administrator is unable to do this
B. In the Management Console
C. In the CLI
D. In the Visual Policy Manager
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51 Which section of the sysinfo file displays information such as the number of successes and failures? (Choose the best answer.)

A. System state statistics
B. Logs
C. Snapshots
D. Health check statistics

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52 What is a series of sysinfo files gathered at periodic intervals called? (Choose the best answer.)

A. Core image dump
B. Event logs
C. Snapshot
D. Minicontext

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 Which process should never be configured on external DNS servers? (Choose the best answer.)

A. Bypass the ProxySG's cache
B. Use DNS imputing
C. Perform lookups on internal servers
D. Perform reverse DNS lookups

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54 Which SGOS edition is designed for Secure Web Gateway hardware deployments? (Choose the best answer.)

A. Proxy Edition
B. Premium Edition
C. MACH5 Edition
D. Basic Edition

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55 What does the authentication mode specify? (Choose the best answer.)

A. The challenge type and the accepted surrogate
B. The protocol used to communicate with the authentication server
C. The time-to-live for credentials
D. Whether the credentials will be encrypted

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56 Which two (2) environments will IP surrogate credentials NOT work in? (Choose two.)

A. With devices that use Network Address Translation
B. Out-of-path deployments
C. Transparent deployments
D. Explicit deployments
E. Multi-user environments such as Citrix

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57 Which section of the sysinfo file would an administrator examine to see how specific components are behaving? (Choose the best answer.)

A. Configuration
B. Logs
C. System state
D. Statistics

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which deployment method represents a single point of failure? (Choose the best answer.)
A. Explicit
B. Basic
C. Transparent
D. Inline

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59 What results when the ProxySG bypasses traffic in explicit mode? (Choose the best answer.)

A. An exception message is displayed to the user
B. Only the default policy can be applied
C. The traffic is redirected
D. Policies are unable to be applied

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 In which type of physical deployment does a ProxySG have potential visibility to all traffic through the use of a device such as WCCP-capable router or a Layer 4 switch? (Choose the best answer.)

A. Transparent
B. Explicit
C. Layer 4
D. In-path

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61 What are two (2) methods by which the ProxySG can detect the type of a file that is downloaded? (Choose two.)

A. Checking the HTTP cache
B. Performing an anti-virus scan
C. Checking the file extension
D. Submitting the URL to WebPulse
E. Detecting apparent data type

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
QUESTION 62 Which VPM layer can be most commonly used to control decrypting of SSL traffic by authenticated username? (Choose the best answer.)

A. SSL Authentication layer
B. Web Authentication layer
C. SSL Intercept layer
D. None of these answers

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 63 How do policy checkpoints evaluate the installed policy on a ProxySG? (Choose the best answer.)

A. At each checkpoint, a decision is made whether to allow or deny the transaction
B. The Server In checkpoint decides which rules will be evaluated by the other checkpoints
C. Relevant rules are evaluated at each checkpoint based on the information about the transaction that is available at that pointD. The Client In checkpoint decides which rules will be evaluated by the other checkpoints

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64 What needs to be enabled for the Explicit HTTP service to be able to hand off SSL traffic? (Choose the best answer.)

A. Early Intercept
B. Detect Protocol
C. Port 443
D. Enable ADN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65 Which proxy service intercepts HTTPS traffic when browsers point directly to the ProxySG and Detect Protocol is enabled? (Choose the best answer.)

A. SSL
B. Explicit HTTP
C. HTTPS
D. TCP Tunnel

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 66 What does the SSL Proxy do by default? (Choose the best answer.)

A. Scans traffic for malware
B. Blocks encrypted traffic
C. Tunnels all HTTPS traffic
D. Intercepts all HTTPS traffic

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 67 When does the ProxySG establish an Schannel? (Choose the best answer.)

A. When the client sends an NTLM type 2 message to the ProxySG
B. When a client request is first received
C. When IWA authentication fails
D. When the client sends an NTLM type 3 message to the ProxySG

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68 When are software workers created during an interaction between a ProxySG and a client requesting a webpage? (Choose the best answer.)

A. At the ProxySG's initial configuration
B. When SGOS receives a connection request
C. When the ProxySG first boots up
D. When a transaction request must be fulfilled from the Internet rather than from the cache

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69 Which two (2) methods are recommended to solve Schannel congestion? (Choose two.)

A. Use Kerberos authentication.
B. Use origin-cookie-redirect credentials.
C. Use special purpose agents.
D. Use NTLM credentials.
E. Use IP surrogate credentials.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70 Which detection method would detect a mismatch between the file name and its content type? (Choose the best answer.)

A. Checking the MIME type
B. Checking the file extension
C. Checking the protocol type

D. Inspecting the file signature

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: