IBM

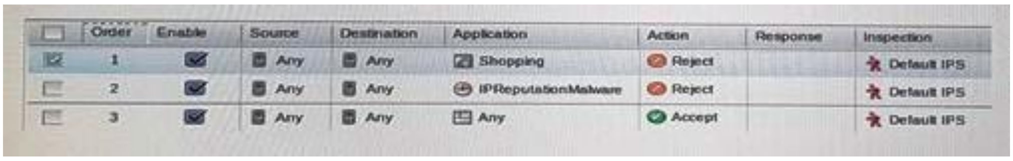
C2150-620

IBM Security Network Protection (XGS) V5.3.2 System Administration

C. Use a Web application object with the stream/download action for the website
D. Use a URL Category object with the News / Magazine category enabled and a Non-Web application with video streaming protocols

Answer: D

QUESTION: 53
A System Administrator has heard that many shopping web sites are infected due to a new vulnerability affecting shopping cart modules used by many open source e-Commerce platforms. The vulnerability only affects shopping sites using SSL.
At the System Administrator's organization, all web-based shopping applications are blocked as required by company policy. Rule 1 was already in place to accomplish this. Outbound SSL inspection was also enabled. The System Administrator has added Rule 2 in an attempt to optimize inspection and better enforce company requirements.



□	Order	Enable	Source	Destination	Application	Action	Response	Inspection
☑	1	☑	Any	Any	Shopping	Reject		Default IPS
□	2	☑	Any	Any	IPReputationMalware	Reject		Default IPS
□	3	☑	Any	Any	Any	Accept		Default IPS

Which analysis of this Network Access Policy is correct with regard to packet inspection optimization?

A. Rule 2 is not required, because Rule 1 is already more efficient.
B. Rule 1 is no longer required. Rule 2 protects from infected web sites.
C. Rule 1 is more efficient than Rule 2, but Rule 2 adds a second layer protection.
D. Rule 2 is more efficient than Rule 1. so the order of Rule 1 and Rule 2 should be reversed.

Answer: B

QUESTION: 54
A System Administrator sees a lot of Ping_Swaep events reported as blocked on the network. However, because the Ping_Sweep signature only blocks the ping packet that triggers the event, most of the ping packets are allowed through the XGS.
How can these suspicious packets be effectively blocked from the network?

A. Add a quarantine response to the Ping_Sweep event
B. Add a Network Access Policy rule to reject ICMP traffic
C. Add a catch-all rule to the bottom of the NAP that rejects oil traffic

QUESTION: 55

A System Administrator wants to integrate the XGS product with an existing SIEM deployment. Which configuration changes should be made to ensure that the SlEM product receives information about security attack incidents?

A. Enable Remote IPFix Flow Data Export for an IPS object
B. Enable QRadar format / LEEF format for the Event Log object
C. Add a remote syslog object with the IP address of the SIEM console to all IPS objects in use
D. Add a quarantine response object with the IP address of the SIEM console to the Advance Threat Protection Agent list

Answer: A

QUESTION: 56

A System Administrator wants to send a message to an SNMP Manager on a network where FIPS mode is used for additional security. The requirement is to monitor the link status of the interfaces. Which type of SNMP response object is needed?

A. SNMP V1 Notification Type: Trap, Enable Authentication Checkbox selected, Authentication Type: MD5, Privacy Type: DES
B. SNMP V2, Notification Type: Trap, Enable Authentication Checkbox selected, Authentication Type: SHA, Privacy Type: AES
C. SNMP V3, Notification Type: Trap, Enable Authentication Checkbox selected, Authentication Type: MD5, Privacy Type: DES
D. SNMP V3, Notification Type: Trap, Enable Authentication Checkbox selected, Authentication Type: SHA, Privacy Type: AES

Answer: C

QUESTION: 57

A System Administrator has deployed an XGS. The NAP policy is configured to generate a local log event tor every accepted network connection, for example, the Event Log object is enabled for the default Accept NAP rule. Due to the number of network connections, the administrator is concerned that this could take up too much disk space on the XGS. Which configuration should the Administrator change to ensure that this does not happen?

A. The Event Log object should be deleted and recreated with a new storage limit
B. The Event Log object should be edited and the percentage of the total event storage limit used for NAP events should be set.
C. The Event Log object should be cloned and the new object should have the percentage of the total event storage limit for all logs set.
D. The Event Log object should be cloned and the new object should only have NAP event logging enabled and the percentage of the total event storage limit used for events should be set.

Answer: C

QUESTION: 58
A System Administrator wants to configure an XGS so that only when the SQL_lnjection security event is enabled in the IPS policy and triggered, the XGS performs a packet capture of the complete connection from the point of the event triggering. How should the System Administrator configure the XGS?

A. Edit the SQL_lnjection security event within the IPS policy and apply a response to capture the connection
B. Edit the I PS object that contains the SQL_lnjection security event and apply a response to capture the connection
C. Create a Network Access policy object with a capture connection response object for the SQL_lnjection security event
D. Create an I PS Filter Policy object for the SQL_lnjection security event and apply a response to capture the connection

Answer: C

QUESTION: 59
Security Policies of an organization demand that no network traffic should be allowed by XGS without inspection in case of XGS power failure or traffic beyond XGS capabilities. What should be the settings for built-in Hardware Bypass and Unanalyzed Policy?

A. Hardware Bypass Mode=Fail Open ; Unanalyzed Policy= Drop
B. Hardware Bypass Mode=Fail Open ; Unanalyzed Policy= Forward
C. Hardware Bypass Mode=Fail Closed ; Unanalyzed Policy= Drop
D. Hardware Bypass Mode=Fail Closed ; Unanalyzed Policy= Forward

Answer: D

QUESTION: 60
A System Administrator is planning to implement SSL Inspection for both outbound user traffic and inbound traffic to a company web server.
The requirements are as follows:
*SSL Inspection should protect users from connections to fraudulent servers
*Outbound SSL Inspection should be limited to select web site categories
*Avoid having to deploy files, configurations, or certificates to User workstations The steps to implement this plan are as follows:
*Obtain an SSL Inspection license for the XGS
*Obtain a certificate from a public CA and upload it to the XGS via Outbound SSL Certificates
*Obtain the certificate and private key of the internal web server and upload it to the XGS via Inbound SSL Certificates
*Add internal CA certificates for the company intranet to the Trusted Certificate Authorities tab in Outbound SSL Inspection Settings
*Configure Outbound SSL Inspection Settings to block connections if the server certificate is self-signed or invalid
*Create Outbound SSL Inspection rules that inspect only specific Domain Certificate Categories
*Create Inbound SSL Inspection rules that only decrypt traffic destined for the internal web server IP address What will happen if an internal user attempts to access the company intranet?

A. The connection will be blocked.
B. The connection will be successful and traffic will be decrypted.
C. The connection will be successful and the traffic will be blocked.
D. The connection will be successful and the traffic will not be decrypted.

Answer: C