IBM

Exam C2150-620

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

Verson: Demo

[Total Questions: 10]

Question No : 1

A System Administrator needs to reinstall and XGS 4100 device.

Which process step is required?

A. Create a bootable image from the file ISNP_5.3.2.3_20160526-0332.pkg
B. Create a bootable image from the file ISNP_5.3.2.3_20160526-0332.img
C. Create a bootable image from the file GX4000.4.6.2_2014.0609_01.40.11. usbimg
D. Create a bootable image from the file GX4000bootsrv.4.6.2_2014.0609_01.40.11 iso

Answer: B

Explanation:

Question

How do you reimage the XGS appliance using a USB drive?

Answer

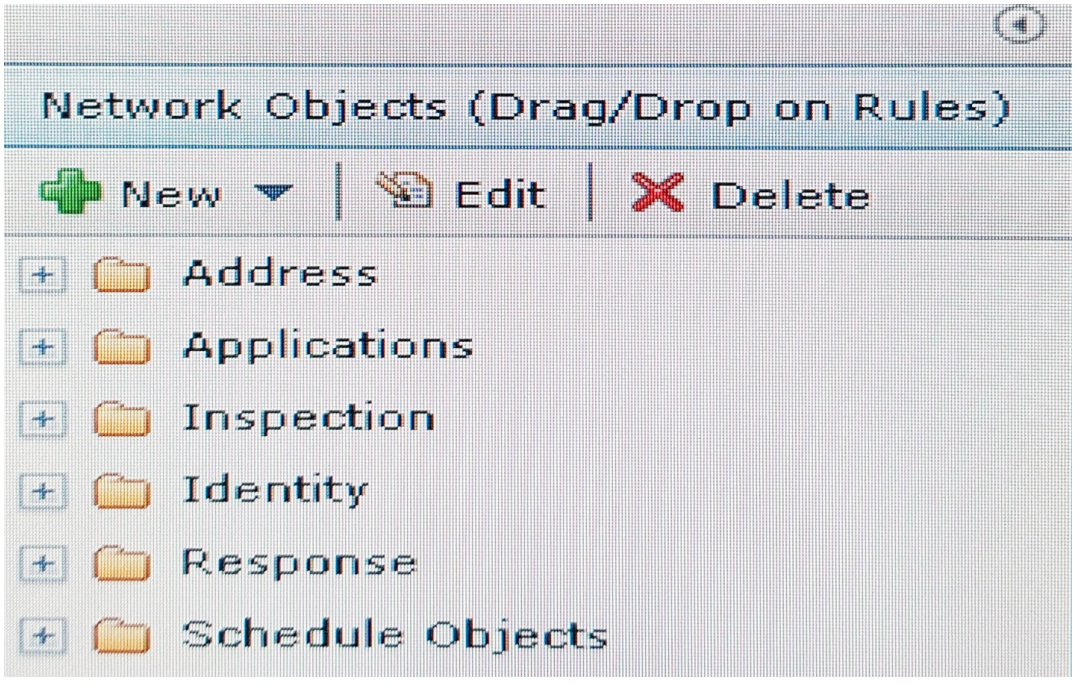
This process applies to any XGS appliance model and the below steps are for the reimage via the USB device. The reimage can be done at any version using the firmware packages available on the IBM Download Center.

Reimaging the IBM Security Network Protection appliance erases all the data from the system and returns it to the unconfigured factory default settings.

References: http://www-01.ibm.com/support/docview.wss?uid=swg21685000

Question No : 2

A financial company bought an XGS appliance to protect the servers running online trade applications. One XGS is just deployed in the staging environment and the initial setup configuration was done; all Security Policies are factory-default. A junior System Administrator accesses the Local Management Interface and opens the Network Access Policy page, and notices that Network Objects can be Drag/Drop on Rules as in the diagram:



Which three actions can be performed using Drag/Drop? (Choose three.)

A. Drag Address folder and drop on Source column of a rule
B. Drag Identity folder and drop on Destination column of a rule
C. Drag Inspection folder and drop on Inspection column of a rule
D. Drag Response folder and drop on response column of a rule
E. Drag Applications folder and drop on Application column of a rule
F. Drag Schedule Objects folder and drop on Schedule column of a rule

Answer: A,C,E

Explanation:

Based on the the attributes Source address, Destination Address, Application, and Inspection, the
Network Access Policy allows for Protection Domains and Connection Events to be configured in XGS.

References: Implementation Guide for IBM Security Network Protection ('XGS for Techies') second edition, Version 2.0, page 21

Question No : 3

A System Administrator of a banking organization has become aware of some malicious traffic to its IBM Security Network Protection (XGS) appliance. The logs show patters of Denial of Service (DoS) attack and a lot of encrypted packets targeted to the M.1 port of the XGS appliance coming from an internal laptop IP address.

What should the System Administrator do next?

A. Configure Management access policy to restrict access.
B. Configure Inbound SSL policy to inspect and drop such traffic.
C. Configure Management access policy to set the management port as TCP reset port.
D. Configure Network access policy and Intrusion Prevention Policy to block DoS attacks.

Answer: B

Question No : 4

A System Administrator has reviewed recent changes on the XGS from the Local Management Interface (LMI) and has determined that a fix pack has been applied that may be inhibiting network functionality. The System Administrator plans to remove the fix pack during the next change control window.

Which step should be taken?

A. Use the Fix Packs page in LMI.
B. Use the Firmware Settings page in the LMI.
C. Use the Command Line Interface command: firmware rollback.
D. Use the Command Line Interface command: fixpacks rollback.

Answer: D

Explanation:

Fixpacks command include rollback, which uninstalls the most recently installed fix pack.

References:
https://www.ibm.com/support/knowledgecenter/en/SSHLHV_5.3.2/com.ibm.alps.doc/references/alps_command_line_interface.htm

Question No : 5

A Security Administrator wants to enable a block page to alert users when they attempt to access HTTP websites that are blocked due to a Network Access policy (NAP) rule.

How should the Administrator achieve this?

A. Add a NAP rule with an action of Drop.
B. Add a NAP rule with an action of Reject.
C. Add a NAP rule that has an action of Do Not inspect and then set the response object to Block Page.
D. Add a NAP rule with an action of Reject (Authenticate) and then create a special user group that has default action of Block HTTP.

Answer: C

Question No : 6

One XGS appliance was deployed on the network edge in a financial company. The 5th rule of Outbound SSL Inspection Policy, Any-Any-Any-Inspect, is enabled. The Outbound SSL Certificate is also imported into the web browser of employees' workstations. The System Administrator found that most HTTPS traffic can be inspected except some that use SPDY protocol.

What should the System Administrator do if all HTTPS traffic must be inspected?

A. Instruct the employees to disable SPDY on their web browser.
B. Add one Advanced Tuning Parameter network. http.spdy.enabled= false.
C. On the Destination tab of the Outbound SSL Rule, select Disable SPDY checkbox.
D. On the Generation Configuration tab of the Outbound SSL Rule, select Disable SPDY checkbox.

Answer: A

Explanation:

Problem(Abstract)

Certain web browser versions use the SPDY protocol to communicate with certain web sites. The Outbound SSL feature in IBM Security Network Protection version 5.3.1 does not support this protocol.
Resolving the problem
IBM has no current plans to support SPDY, due to the fact that the protocol has been deprecated in favor of HTTP 2.0. Use the following instructions to disable the SPDY protocol for browsers that support it.

Chrome
Execute the following command to start Chrome:
<installed path of Chrome>\chrome.exe --use-spdy=off

FireFox 37

Internet Explorer 11 with Windows 8.1

Note: SPDY is an now-deprecated open-specification networking protocol that was developed primarily at Google for transporting web content.[1] SPDY manipulates HTTP traffic, with particular goals of reducing web page load latency and improving web security.

References: http://www-01.ibm.com/support/docview.wss?uid=swg21903522

Question No : 7

An Administrator has just configured a new XGS appliance to run in FIPS mode. After deploying the company policies to the appliance, the Administrator realizes the User Authentication feature is not working.

What is the likely cause of the problem?

A. The appliance was not restarted.
B. TLS 1.0 and 1.1 are not enabled.
C. The FIPS integrity check failed to run.
D. User Authentication is not supported in FIPS mode.

Answer: B

Explanation:

If you enable FIPS mode on your appliance and plan to use the user authentication feature, you must enable TLS 1.0 and TLS 1.1 during the FIPS configuration process to enable the use of Mozilla Firefox or Google Chrome browsers. You do not need to enable TLS 1.0 and TLS 1.1 if all of your network users use Microsoft Internet Explorer.

References:
https://www.ibm.com/support/knowledgecenter/en/SSHLHV_5.3.2/com.ibm.alps.doc/tasks/alps_enabling_fips_mode.htm

Question No : 8

A System Administrator has deployed an XGS. The NAP policy is configured to generate a local log event for 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: B

Explanation:

By default, the maximum storage space for events is set to 2048 MB (2 GB). Events are stored in a database, which estimates the size of each event at 500 bytes, which means the database can store a maximum of 4,096,000 events.
You can distribute the maximum events among different event types. When the event count

for an event type exceeds 90% of the maximum event allocation, older event data is erased and overwritten.

Note:
You can adjust the maximum size using the following tuning parameter:
Key: events.response.logdb.disklimit
Value: 2048
The default value is 2048 MB (2 GB). To increase the maximum size to 4 GB, change the value to 4096.

References: Implementation Guide for IBM Security Network Protection ('XGS for Techies') second edition, Version 2.0

Question No : 9

A Security Administrator want to block access to streaming video on a news website.

Which object should be used and how should it be configured?

A. Use an IP Reputation object with the streaming video option enabled.
B. Use a URL Category object with the News/Magazine category enabled.
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: C

Explanation:
Use Web Application objects to control access to categorized types of web-based applications and to control how people use them on your network. The Network Protection database provides an indexed list of Web Application categories that you can block or limit access to on your network. These categories include web mail, social networking, and gaming sites.
In addition to blocking or limiting these site categories, you can prohibit users from performing specific actions on many of these sites. You can allow users to view social media sites such as YouTube or Flickr, but not allow users to post to them. Or you can

allow users to view and to post to networking sites, such as Facebook or Myspace, but not to upload photos or to play games.

Example: Block video on cnn.com
On the Web Applications tab, click the Filter button and create a filter.
The Filter returns a list of Web Applications with news content and the associated Actions.
Add cnn.com – Stream/Download to the Added Web Application Actions list. Click Save Configuration.
Etc.

References: Implementation Guide for IBM Security Network Protection ('XGS for Techies') second edition, Version 2.0, pages 74-78

Question No : 10

A System Administrator has configured SSL Inspection in XGS, but end users get promoted to verify the certificate in the browser when viewing SSL web pages. To fix the issue the System Administrator must distribute the CA certificates so that it can be imported in the Trusted Root Certification Authorities in end users' browsers.

Which Menu option allows the System Administrator to download the CA Certificate?

A. Inbound SSL Certificates
B. Appliance SSL Certificate
C. Outbound SSL Certificates
D. Management Certificate Authorities

Answer: C

Explanation:
In order for Outbound SSL to work properly, the XGS Certificate Authority (CA) certificate must be installed in the browser in order for the browser to verify the identity of the XGS. If you do not add the CA certificate, Outbound SSL will not work properly, introduce latency, and could cause pages to fail to load.
If users get prompted to verify the certificate in the browser when viewing SSL web pages,

this indicates that the CA is not loaded or is loaded in the incorrect place. The CA certificate must be loaded in the Trusted Root Certification Authorities tab in Certificates in Internet Explorer and the Authorities tab in the Certificates Manager in Firefox.

To download the CA certificate, log on to the LMI and go to Manage System Settings > Network Settings > Outbound SSL Certificates. Select the Active Device CA certificate and select Download.

References: http://www-01.ibm.com/support/docview.wss?uid=swg21958051