

# EXAMGOOD

## QUESTION & ANSWER

Exam Good provides update free of charge in one year!

Accurate study guides  
High passing rate!

<http://www.examgood.com>

**Exam : C2150-620**

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

**Version : DEMO**

1.A System Administrator has been seeing a lot of SSLv2\_Weak\_Cipher attacks reported on the network and wants to Increase the severity of the events.

How can this be accomplished?

- A. Modify the Threat Level of the signature
- B. Create an Incident in SiteProtector for SSLv2\_Weak\_Cipher
- C. Modify the Event Log response for the Intrusion Prevention Object
- D. Increase the X-Force Protection Level for the Intrusion Prevention Object

**Answer: D**

2.A system Administrator wants to configure an XGS so that when the SSH\_Brute\_Force security event is triggered against machine Server1, any further traffic from the source IP address contained in the security event alert is dropped for a timed period.

How should the System Administrator configure the XGS to perform this?

- A. Edit the properties of the SSH\_Brute\_Force security event and create a quarantine response to block the source IP
- B. Create a Network Access policy object to drop all traffic from the source IP contained in the security event alert to Server1
- C. Create a Network Access policy object with a quarantine rule to block the source IP when the security event is triggered against Server1
- D. Create an IPS Fitter policy object for the SSH\_Brute\_Force security event with a Victim address of Server1 and a quarantine response to block the source IP

**Answer: C**

3.A System Administrator is preparing to manage an XGS appliance using the SiteProtactor System. Which three management actions can be performed? (Choose three.)

- A. Apply a snapshot
- B. Restart the appliance
- C. Configure Static Routes
- D. Create a Firmware backup
- E. Manage the Appliance SSL Certificate
- F. Change the Flexible Performance Level

**Answer: ADE**

4.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 a default action of Block HTTP

**Answer: C**

5.The System Administrator has discovered the XGS device is overloaded and is dropping legitimate

traffic.

Which setting is likely responsible for this behavior?

- A. Unanalyzed policy configuration
- B. TCP resets - TCP reset interface
- C. Fail Closed hardware bypass mode
- D. LogDB response enabled on NAP rules

**Answer: A**