

PASSTCERT

QUESTION & ANSWER

Higher Quality
Better Service!

We offer free update service for one year
[HTTP://WWW.PASSTCERT.COM](http://www.passtcert.com)

Exam : **000-561**

Title : IBM Security Network
Intrusion Prevention System
V4.3 Implem

Version : Demo

1. Where is the provinfo file stored?

- A. /var/cache
- B. /var/support/
- C. root directory
- D. admin directory

Answer: B

2. How is a firewall rule configured to block remote desktop (RDP) access for all interfaces and all Virtual Local Area Networks.?

- A. protocol=TCP, source port exclude RDP
- B. action=ignore, select Interfaces, protocol=TCP, port=3389
- C. keep all default settings but change the target port to 3389
- D. action=drop, protocol=UDP, target port uncheck any and enter 3389

Answer: C

3. Which interface mode is required in order for quarantine response rules to work?

- A. Bypass Mode
- B. Inline Protection Mode
- C. Inline Simulation Mode
- D. Passive Monitoring Mode

Answer: B

4. Where would a user be added to allow a remote user to access the IBM Security Network Intrusion Prevention System V4.3 Local Management Interface?

- A. the Remote Access policy in IBM Security SiteProtector System (SiteProtector)
- B. the User Management utility in SiteProtector
- C. the Accounts and Passwords page in the Web interface
- D. the Password Management menu in the SSH Configuration menu

Answer: C

5. What are two restrictions placed on remote users using IBM Security Network Intrusion Prevention System V4.3? (Choose two.)

- A. They cannot reboot the appliance.
- B. They cannot log in to the local console.
- C. They cannot change the local user account passwords.
- D. They cannot save changes to policies in the Web interface.
- E. They cannot log in to the appliance when the authentication server is down.

Answer: C,E

6. Which file is accessed on the IBM Security Network Intrusion Prevention System V4.3 appliance to determine why it is Active with Errors in IBM Security SiteProtector System?

- A. Boot log file
- B. Kernel log file
- C. Engine0 log file

D. Messages log file

Answer: D

7.Which area of the IBM Protocol Analysis Module technology prevents Skype from using enterprise network bandwidth?

- A. Data Security
- B. Application Control
- C. Threat Detection and Prevention
- D. Client-side Application Protection

Answer: B

8.Where in the IBM Security SiteProtector System Console can a customer find the link status of the Security Interfaces on an IBM Security Network Intrusion Prevention System appliance?

- A. the networkinfo section under Module Status in the appliance Properties screen
- B. the Intrusion Prevention section under Module Status in the appliance Properties screen
- C. the Security Interfaces section on the Health Summary Network tab in the appliance Properties screen
- D. the Internal Communication section on the Health Summary System tab in the appliance Properties screen

Answer: A

9.A customer wants to change the severity of an IBM Protocol Analysis Module signature from high to low in a given protection domain. Which policy meets this requirement?

- A. Security Events
- B. Open Signatures
- C. System Updates
- D. X-Force Virtual Patch

Answer: A

10.Where in the Local Management Interface is the location of the date and time of the last backup of an IBM Security Network Intrusion Prevention System V4.3 viewable?

- A. Evidence log
- B. Message log
- C. System Dashboard
- D. Security Dashboard

Answer: C

11.What are two purposes for the Quarantine Rules in the Response Tuning page in the Local Management Interface? (Choose two.)

- A. add new quarantine rules
- B. set network configuration options
- C. temporarily disable a quarantine rule
- D. review rules generated in response to intruder events
- E. define how the appliance should send notifications when it detects an intrusion in the network

Answer: A,D

12.Which file can be imported or compiled, and defines the format of SNMP traps for security events responses in the IBM Security Network Intrusion Prevention System appliance?

- A. iss.mib
- B. ibm.mib
- C. linux.mib
- D. snmp.mib

Answer: A

13.Which two user notification response object types are available in IBM Security Network Intrusion Prevention System V4.3? (Choose two.)

- A. SMS
- B. E-mail
- C. Remedy
- D. Voicemail
- E. SNMP Trap/Inform

Answer: B,E

14.Log Evidence is enabled for an event and an administrator wants to review the packet content. Where in the Local Management Interface is this log file downloaded?

- A. under Security Settings, select the policy that logs the event, click on Download Log, and the save file
- B. select Review, under Downloads select Logs and Packet Captures, select the files, and click Download
- C. on the Security Dashboard, click the Evidence Logs link, click all files related to the event, and save the files
- D. select Home Dashboard, scroll down to the section on evidence logs, select the log file(s), and click Download

Answer: B

15.Virtual Local Area Network (VLAN) exclusions have been added to a Protection Domain, however events from those VLANs seem to be generated anyway. What is the most likely cause?

- A. A VLAN cannot be excluded in a custom Protection Domain.
- B. Multiple VLANs cannot be excluded in a custom Protection Domain.
- C. Incorrect interfaces have been specified in a custom Protection Domain.
- D. The same exception has not been created on the Global Protection Domain.

Answer: C