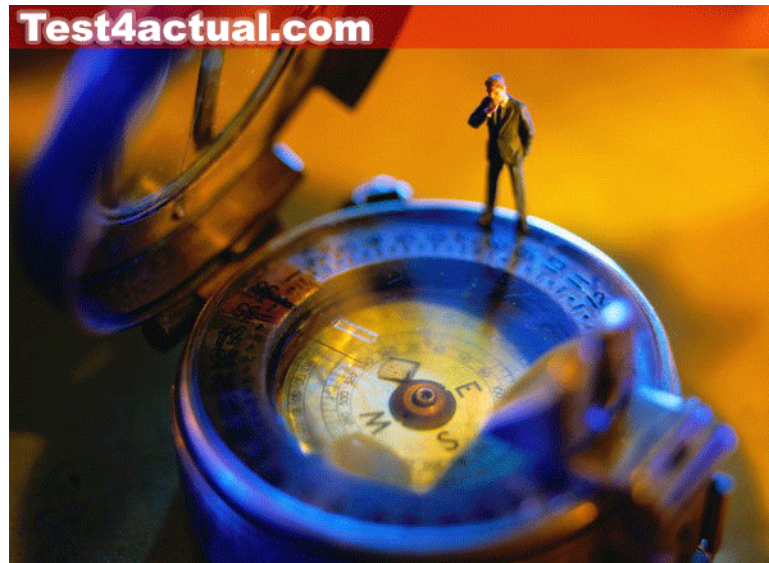


Test4actual, 100% Accurate Answers!!!



Help you pass any IT exam!

HP HP0-J16

Introduction to HP SANs

Q&A DEMO

English: www.Test4actual.com

BIG5: www.Test4actual.net

GB: www.Test4actual.cn

www.test4actual.com

1. What are default alerts when installing ProCurve NIM? (Select two.)

- A.default SNMP alert
- B.default ProCurve alert
- C.default Duplicate IP alert
- D.default Virus Throttle alert
- E.default Packet Size Deviation alert

ANSWER: DE

2. What is an appropriate response to an alert triggered by a Duplicate IP event?

- A.MAC Lockout
- B.Port Rate Limit
- C.Email Notification
- D.Quarantine VLAN

ANSWER: C

3. Where in PCM+ can you view a graph of the number of alerts received over time?

- A.Dashboard tab
- B.security heat map
- C.Security Activity --> Alerts tab
- D.Security Activity --> Offenders tab

ANSWER: A

4. You have configured a policy that matches the Port Disable action to a TCP/UDP Fanout alert. Which statement is true?

- A.The TCP/UDP fanout alert is not intended for triggering threat mitigation actions.
- B.The Port Disable action should always be accompanied by the Port Mirror action.
- C.A port scan targeted against a server can cause the server to trigger the TCP/UDP alert.
- D.The TCP/UDP Fanout alert tracks endpoints by MAC address, so MAC Lockout is a better action.

ANSWER: C

5. How does a ProCurve Network Immunity Solution protect a network?

- A.It deals with threats from authorized users.
- B.It stops unauthorized users from connecting.
- C.It customizes users' rights based on their identity.
- D.It filters Web content and email while searching for viruses.

ANSWER: A

6. How can ProCurve NIM mitigate threats?

- A.It sends out messages to reset offenders TCP sessions.
- B.It sends traps to external IPSs and has them mitigate the threats.
- C.It executes actions on the device through which the offender connects.
- D.It drops the offending traffic, protecting the resources installed behind NIM.

ANSWER: C

7. What is a feature of anomaly-based threat detection but not signature-based threat detection?

- A.detecting worms
- B.detecting DoS attacks
- C.detecting protocol anomalies
- D.detecting undocumented attacks

ANSWER: D

8. Which threat detection method compares traffic to a baseline of normal activity?

- A.host-based
- B.user-based
- C.anomaly-based
- D.signature-based

LAN

ANSWER: C

9. What is the standard name for a device that includes a firewall, Web content filtering, and antivirus capabilities?

- A.Network Immunity Solution (NIS)
- B.Intrusion Detection System (IDS)
- C.Intrusion Prevention System (IPS)
- D.Unified Threat Management (UTM)

ANSWER: D

10. A network already has an Intrusion Prevention System (IPS) that is installed between a group of servers and the rest of the network. Which benefits does ProCurve NIM add in a NIM + IPS deployment? (Select two.)

- A.deep packet inspection
 - B.signature-based detection
 - C.remediation of infected endpoints
 - D.protection for other resources throughout the network
 - E.applies actions closer to the point of origin of the attack
- ddress, so MAC Lockout is a better action.

ANSWER: DE

11. When should the NIM + inline IPS deployment option be used?

- A.to allow ProCurve NIM to apply configuration changes to non-ProCurve devices
- B.to take immediate action to protect key resources and also to track threats to the source
- C.to allow ProCurve NIM to mirror suspicious traffic to an external device for more analysis
- D.to add threat protection to the features of ProCurve NIM, which include only threat detection

ANSWER: B

12. When should the unified NIM + IDS deployment option be used?

- A.to take immediate action to protect key resources and also track threats to the source
- B.to add threat protection to the features of ProCurve NIM, which include only threat detection

- C.to allow ProCurve NIM to mirror suspicious traffic to an external device for additional analysis
- D.to protect against threats from wireless devices, which ProCurve NIM is not able to do on its own

ANSWER: C

13. Which challenges does a unified NIM + IDS deployment meet? (Select two.)

- A.reducing false positives
- B.managing remediation and patch deployment
- C.managing antivirus signature updates for ProCurve NIM
- D.dropping threats as they travel into a secure part of the network
- E.minimizing the overhead caused by mirroring through the dynamic activation of mirrors

ANSWER: AE

14. Which features are provided in a ProCurve NIM standalone deployment? (Select two.)

- A.threat mitigation without the aid of PCM+
- B.resetting of TCP sessions when threats are detected
- C.signature-based detection of worms and other attacks
- D.applying mitigation actions near the source of the threat
- E.application of different policies based on the threat's place of origin

ANSWER: DE

15. Click the Exhibit button.

ProCurve NIM is failing to dynamically mirror traffic to an IDS. You check the mirror on the switch that connects to the offender. Based on the information in the exhibit, what could be causing the problem with mirroring?

- A.No port has been configured as a mirror destination.
- B.The SNMP settings on the switch, to which the IDS connects, do not match the settings of PCM.
- C.The Find Node tool has failed to locate the offender, so ProCurve NIM cannot execute the action.
- D.The manager password on the switch to which the offender connects does not match the settings of PCM.

ANSWER: A

16. Which misconfiguration on PCM+ causes ProCurve NIM to fail to detect any anomalies in traffic?

- A.the wrong sFlow version
- B.an incorrect operator password
- C.an incorrect manager password
- D.an incorrect SNMP community name

ANSWER: D

17. A network has 400 devices, 375 of which support sFlow/XRMON. The PCM+ server manages 350 ProCurve

devices, 335 of which support sFlow/XRMON. How many device licenses does ProCurve NIM

require?

- A.335
- B.350
- C.375
- D.400

ANSWER: B

18. What is the intended purpose of the default traffic sampling action of ProCurve NIM?

- A.to prevent ProCurve NIM from triggering false positives
- B.to help PCM+/NIM periodically begin to monitor new ports
- C.to send traffic for increased analysis to an Intrusion Detection System (IDS)
- D.to allow ProCurve NIM to take immediate action against the most probable threats

ANSWER: B

19. Which statement is true about the default behavior of ProCurve NIM after installation?

- A.NIM logs events and alerts and can change device configurations.
- B.NIM logs events and alerts but does not change device configurations.
- C.NIM logs events, but not alerts, and does not change device configurations.
- D.NIM does not log events or alerts and does not change device configurations.

ANSWER: B

20. You want to track the complete process of threat detection and mitigation in a NIM + IDS deployment. How should you search for the relevant events?

- A.Type NBAD for the Source filter in the Interconnect Devices Events tab.
- B.Type NBAD for the Source filter in the Network Management Home Events tab.
- C.Type Policy Manager for the Source filter in the Interconnect Devices Events tab.
- D.Type Policy Manager for the Source filter in the Network Management Home Events tab.

ANSWER: D