

# ***KillTest***

Higher Quality, Better Service!



## **Q&A**

<http://www.killtest.com>

We offer free update service for one year.

**Exam** : **HP0-Y16**

**Title** : ProCurve Network Immunity  
Solutions

**Version** : Demo

1. Which alert can be triggered by SNMP traps sent by ProCurve switches?

- A. default External
- B. default IP Fanout
- C. default IP Spoofing
- D. default Virus Throttle
- E. default ProCurve SNMP

**Answer: D**

2. How do you configure PCM+ to generate periodic reports?

- A. Select the Reports button in the global toolbar.
- B. Enable the periodic reports setting in PCM+ Preferences.
- C. Configure the schedule in the appropriate Reports Wizard.
- D. Create policies with schedule-driven alerts and report actions.

**Answer: D**

3. What is a reason to create a custom group for a server zone and set that group as the source for a NIM policy?

- A. Servers handle more mission-critical traffic, so you set less drastic actions.
- B. Servers trigger more false positives, so you set the NBAD sensitivities lower.
- C. Threats are targeted to servers at all times, so you set the policy to any time.
- D. Threats that are targeted to servers are more serious, so you set harsher actions.

**Answer: A**

4. 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**

5. What should you do to set up your network infrastructure for remote mirroring?

- A. Enable jumbo frames.
- B. Enable frame fragmentation.
- C. Raise the maximum transmit unit (MTU).
- D. Reserve uplink ports for the mirroring session.

**Answer: A**

6. 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**

7. You want to display and print a list of all events related to the Policy Manager. What should you do?

- A. From the Reports menu, select the Policy Events report.
- B. In Interconnect Devices, click the Events tab; filter for Policy Manager; click the Print button.
- C. From the Reports menu, select the Events report; filter for Policy Manager in the Report Wizard.
- D. In Network Management Home, click the Events tab; filter for Policy Manager; click the Print button.

**Answer: D**

8. Your company's regulatory compliance group has asked you for a record of changes to the Policy Manager policies. Which report should you generate?

- A. Security Audit
- B. Actions by Policy
- C. Executed Policies
- D. Automation (Policy) History

**Answer: C**

9. 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

10. Which action can help you troubleshoot a policy in realtime from PCM?

- A. Port Mirror
- B. Notify (Email)
- C. Message Dialog
- D. Traffic Sampling

**Answer:** C

11. 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

**Answer:** DE

12. How does ProCurve NIM determine the severity level for a security alert?

- A. from the violation count for the associated event
- B. from the event, and the severity cannot be overridden
- C. from the event, unless overridden by the alert configuration
- D. from the event for trap events and from the alert configuration for other events

**Answer:** C

13. Which events can be signs of an unauthorized port scan? (Select two.)

- A. Port Anomaly
- B. DNS Tunneling
- C. TCP/UDP Fanout
- D. UDP Protocol Anomaly
- E. TCP Protocol Anomaly

**Answer: CE**

14. ProCurve NIM was registering few TCP/UDP Fanout events. You have raised the sensitivity, and many false positive TCP/UDP Fanout events are now triggered throughout the network. What should you do next? (Select two.)

- A. Lower the sensitivity to the previous level.
- B. Remove the TCP/UDP alert from all policies.
- C. Plan and create a Policy Manager policy to deal with false positive events.
- D. Exclude the devices triggering the false positive events from the TCP/UDP fanout.

**Answer: AD**

15. By default, which NBAD event will trigger traffic sampling on a port?

- A. Duplicate IP
- B. Virus Throttle
- C. Protocol Anomaly
- D. Packet Size Deviation

**Answer: D**

16. 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**

17. What might indicate that the sensitivity for IP fanout has been set too high?

- A. IP Fanout events appear in the Events tab for almost every switch.
- B. Although you do not see IP Fanout events, the IP Fanout alert triggers.
- C. IP Fanout events appear in the Events tab for one switch but not others.
- D. There are no IP Fanout events for days although you have configured an IP Fanout alert.

**Answer: A**

18. Which threat mitigation action is supported on ProCurve wireless devices?

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

**Answer: B**

19. 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**

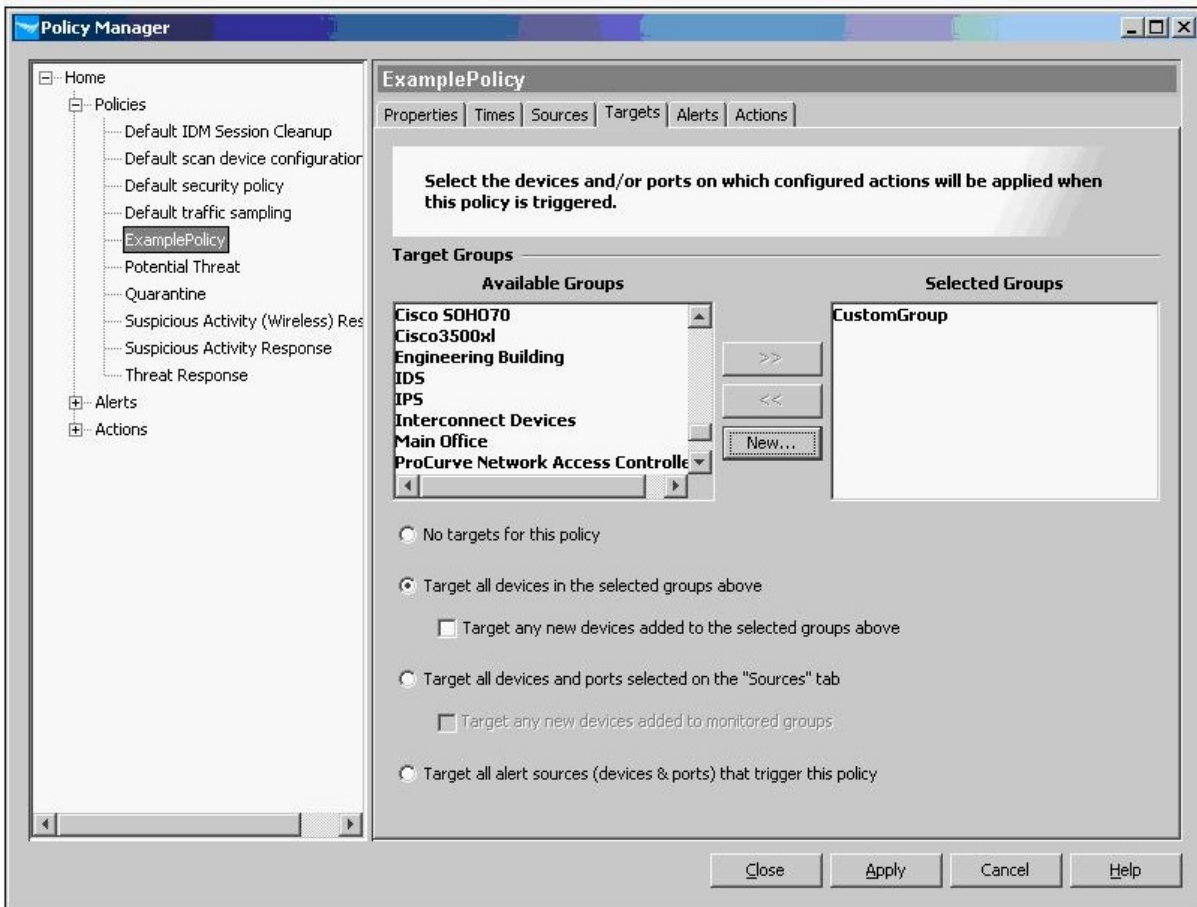
20. Which tab is added to PCM+ when you install ProCurve NIM?

- A. Policy Events
- B. Security Audit
- C. Event Browser
- D. Security Activity

**Answer: D**

21. Click the Exhibit button.

What are reasons to configure the policy settings shown in the exhibit? (Select two.)



- A. You want the policy to respond to threats from offenders within this group.
- B. You want ProCurve NIM to apply the policy for threats detected in this group.
- C. You have set the policy to a source group, so you must set the target group to match.
- D. You want to enable dynamic local port mirroring on set ports, which compose this group.
- E. The policy action is MAC Lockout, and you want to lock the offender out of the entire group.

**Answer: DE**

22. You want to set up different external alerts based on the specific type of threat. Which settings can help you accomplish this task? (Select two.)

- A. Trap ID
- B. Severity
- C. Description
- D. Anomaly ID



E. Violation Count

**Answer: AC**

23. 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**

24. Which statement is true about setting up an action for dynamic remote mirroring?

- A. You should configure the mirror source before configuring the action.
- B. You should configure the mirror destination before configuring the action.
- C. You configure both the mirror source and destination as part of configuring the action.
- D. You should configure both the mirror source and destination before configuring the action.

**Answer: B**

25. From which NBAD event should you often exclude your servers?

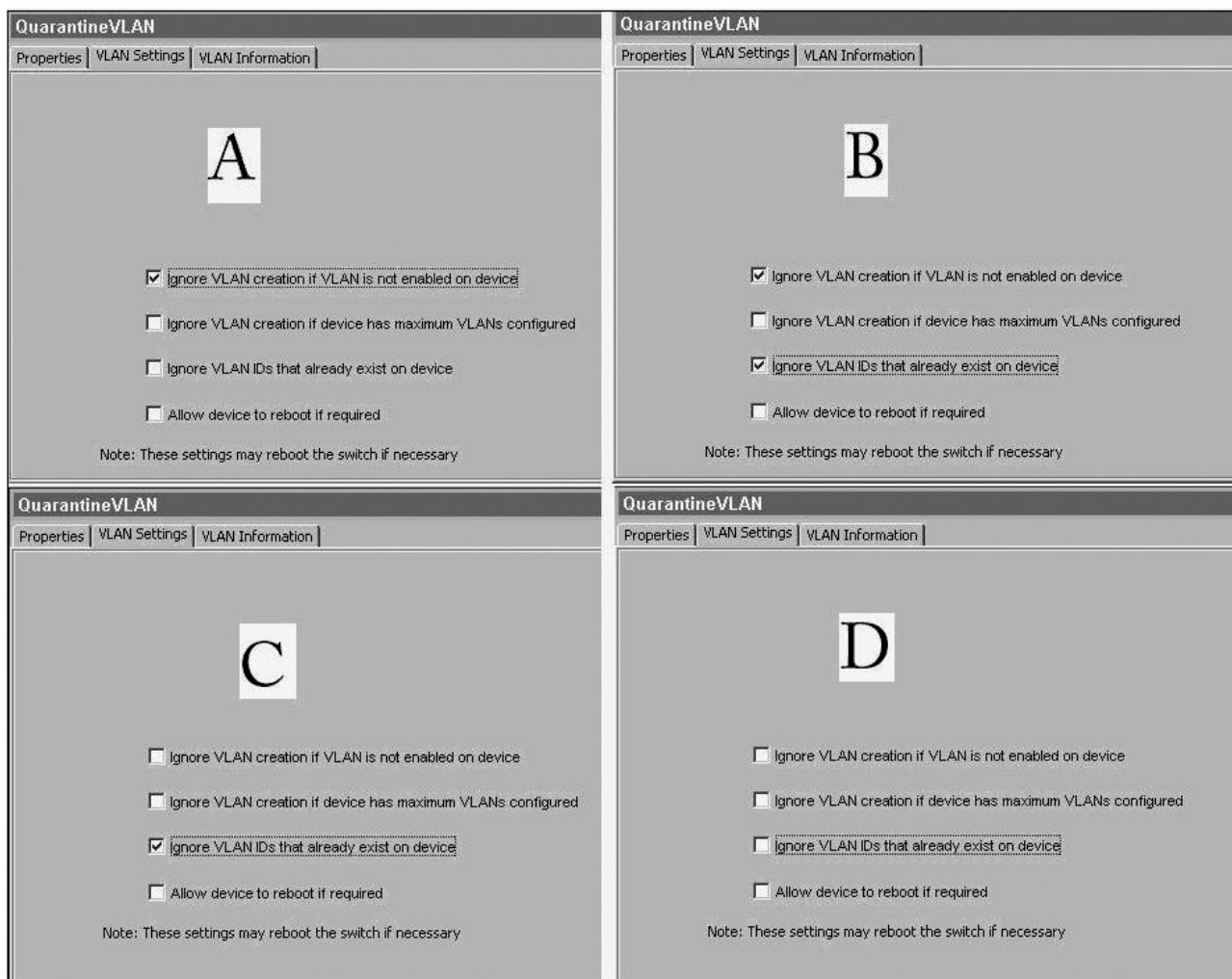
- A. DNS Tunneling
- B. TCP/UDP Fanout
- C. Protocol Anomaly
- D. Packet Size Deviation

**Answer: B**

26. Click the Exhibit button.

You are configuring a Quarantine VLAN action.

Which area in the exhibit displays settings that allow ProCurve NIM to always place the offender in the Quarantine VLAN?



- A. a
- B. b
- C. c
- D. d

**Answer: D**

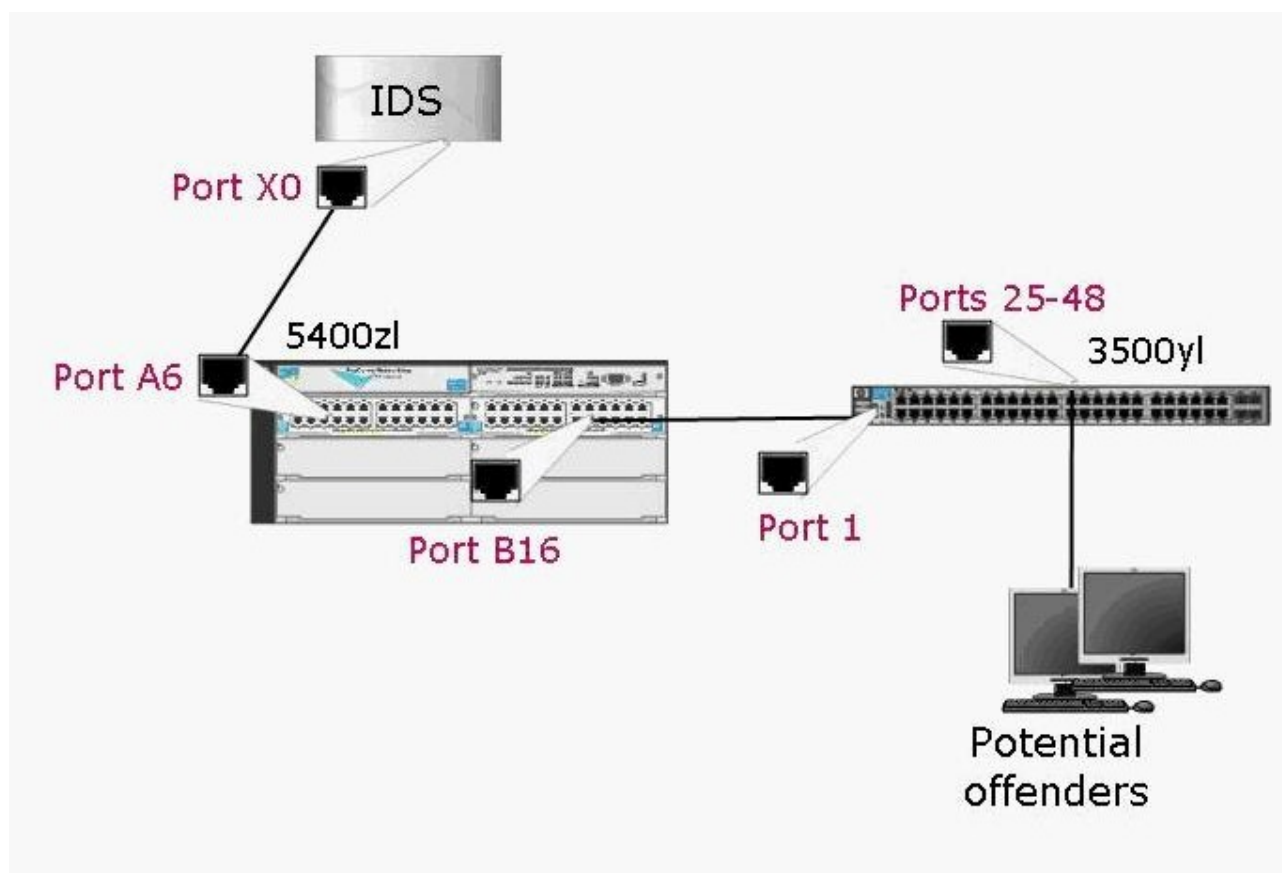
27. What must you do to configure a Port Rate Limit action?

- A. Set the rate limit as a percentage.
- B. Set the rate limit as a QoS priority value.
- C. Set the rate limit as an absolute value in Kbps.
- D. Enable the limit, leaving the rate to be determined by the switch configuration.

**Answer: A**

28. Click the Exhibit button.

Which port in the exhibit should you select in PCM+ and configure as the mirror destination?



- A. 1
- B. A6
- C. X0
- D. B16
- E. 25-48

**Answer: B**

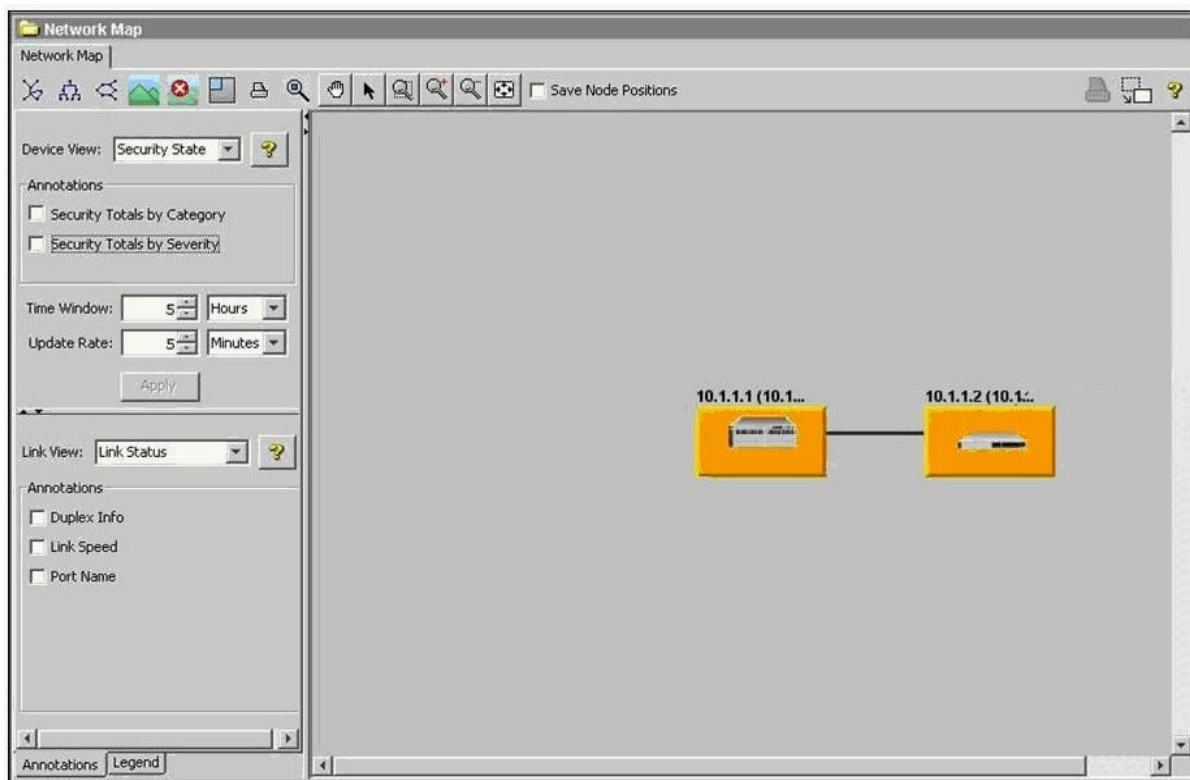
29. Which statement is true about the role that events play in ProCurve NIM?

- A. When a particular event occurs, ProCurve NIM executes the corresponding alert.
- B. When a particular event occurs, ProCurve NIM executes the corresponding policy.
- C. When a particular number of events occur within a set time window, ProCurve NIM triggers the corresponding alert.
- D. When a particular number of events occur within a set time window, ProCurve NIM triggers the corresponding policy.

**Answer: C**

30. Click the Exhibit button.

Given the information shown in the exhibit, what do you know about alerts on the 10.1.1.1 device over the last five hours? (Note: The orange color corresponds with Major severity.)



- A. The device has received only Major alerts.
- B. The majority of alerts on the device are Major alerts.
- C. The highest severity for an alert on this device is Major.
- D. The most recent alert received on the device was a Major alert.

**Answer: C**