



HP Certified Professional Program

ProCurve Network Immunity Solutions,
HP0-Y16

Exam Preparation Guide

Purpose of the Exam Prep Guide

The intent of this guide is to set expectations about the content and the context of the exam and to help candidates prepare for the exam. In this guide, you will find recommended HP training courses, reference and study material to help you achieve a successful passing score.

Studies conducted by HP and Prometric show that a combination of course attendance and self-study maximizes the likelihood of passing the exam on the first attempt.

Audience

This exam is for systems engineers or networking engineers designing complex networks. Examples of job roles:

Reseller and customer network specialists, System Engineers, Network Engineers, HP Field System Engineers, HP Services Technical Support and Field Services Engineers

ProCurve Network Immunity Solutions provides network engineers with the knowledge and skills required to use the ProCurve Network Immunity Manager (NIM) to protect their network from malware, denial of service (DoS) attacks, and other threats. The course provides hands-on experience in configuring and troubleshooting NIM both as a standalone threat detection and threat mitigation solution and as a combined solution with a third-party Intrusion Detection System (IDS).



Certification Requirements

ProCurve Network Immunity Solutions, HPO-Y16, is one of the core requirements to be certified as a Master Accredited System Engineer (ASE) ProCurve Networking Security Specialist [2008].

The Master ASE – ProCurve Networking designation provides certification that an individual has the skills to design complex, scalable ProCurve-based networks and can implement and support complex secure, switched and routed environments. This level of certification establishes the competencies required for hands-on design, integration and support of ProCurve Security Solutions for complex, enterprise networks. Given a set of customer business requirements, a MASE is expected to perform consultative planning, architecting and leading the deployment of secure ProCurve solutions. This may include products and components from other vendors as necessary to solve business needs. Key focus is on understanding the security impacts of applications and network services.

Prerequisites

The following requirements are prerequisites for the Master ASE – ProCurve Networking Security Specialist [2008] Certification.

- AIS – HP ProCurve Networking
- Attend the ProCurve Security v7.31 course and/or pass the associated exam (HPO-Y11)
- Attend the Building ProCurve Resilient, Adaptive Networks v7.41 or later course and/or pass the associated exam (HPO-Y12)
- Attend and/or pass the exam for ProCurve Network Management v8.11 and/or pass the exam for ProCurve Network Management (HPO-Y13)
- Attend and/or pass the exam for ProCurve Network Access Control v8.11 and/or pass the exam for ProCurve Network Access Control (HPO-Y15)
- Attend the ProCurve Network Immunity Solutions v8.21 or later course and/or pass the exam for ProCurve Network Immunity Solutions (HPO-Y16)

Exam Details

At the beginning of the exam, you will be asked to answer several survey questions. The survey questions are designed to assist the exam development team in accurately profiling test results and to improve future exams.

The following are details about the exam:

- **Number of items:** 60
- **Item types:** multiple choice
- **Time commitment:** 90
- **Passing Score:** 75% (45 items to pass)
- **Reference Material:** No on-line or hard copy reference material will be allowed at the testing site.

Comments on the Exam

During the exam, participants can make specific comments about the items (i.e., accuracy, appropriateness to audience, etc). HP welcomes these comments as part of our continuous improvement process.

Exam Content

The following testing objectives represent the specific areas of content covered in the exam. Use this outline to guide your study and to check your readiness for the exam. The exam measures your understanding of these areas.

Objective	
1.0	Explain why a network immunity solution is vital to protecting your network from emerging threats
	Define Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and Unified Threat Management (UTM)
	Describe the four components of the ProCurve Network Immunity Manager (NIM)
	List the three options for deploying the Network Immunity Solution and give reasons for choosing a particular option
	Install ProCurve Manager Plus (PCM+) and NIM, setting initial parameters to support NIM's functions
	Describe how NIM automatically monitors your network

Objective

	with default alerts, actions, and policies
2.0	Describe the three types of events that can trigger an alert in NIM
	<p>Make an educated guess about the type of attack that caused NIM's Network Behavior Anomaly Detection (NBAD) engine to detect a particular anomaly</p> <p>List actions NIM can take and choose appropriate actions to respond to particular alerts</p> <p>Describe the capabilities of various ProCurve switches for supporting NIM</p> <p>Configure alerts and actions and create basic NIM policies</p>
3.0	Set up your network infrastructure for a NIM + IDS deployment
	<p>Set up your third-party IDS to interoperate with NIM</p> <p>Plan and create policies that mirror suspicious traffic to an external IDS</p> <p>Plan and create external alerts and policies that take action based on those alerts</p> <p>Troubleshoot a NIM + IDS deployment</p>
4.0	Use PCM+ tabs, maps, and reports to audit security vulnerabilities, track offenders, refine policies, and support regulatory compliance
	Generate security reports, both manually and automatically
5.0	Establish your baseline and complete the initial network immunity lifecycle
	<p>Analyze security events to establish your security policy</p> <p>Use best practices to create policies customized to your environment</p> <p>Continue to complete the network immunity lifecycle to refine policies</p>

Recommended Training and Study References

This section lists training courses and documents that can help you acquire a majority of the knowledge and skills needed to pass the exam. You must also gain the practical experience outlined in this guide

You are not required to take the courses listed in this section. However, HP **strongly recommends** that you attend the classes, participate in class labs, and thoroughly review all course material and documents before taking the exam, even if you believe you have sufficient on-the-job experience.

Instructor-Led Training

Use the information in this guide and the practical experience you have gained

Title	Course Number	How to Enroll
ProCurve Network Immunity Solutions (v8.21 or later)	00048679	http://www.hp.com/go/procurvetraining use the regional links to find schedules and registration information

Documentation

Title	Section Title	Source/Order Number
ProCurve Network Immunity Manager and related software and switch manuals	All Applicable titles	http://www.hp.com/rnd/support/manuals/index.htm

Other Reference Material

Title	Order Number	Source
FAQs, Manuals, Configuration Examples, etc.		http://www.hp.com/rnd/support/

Exam Registration

For information about exam registration, [click here](#).

Sample Test Items

The following examples represent the types of items and question formats that you could see on the exam.

1. Click the Exhibit button.

The screenshot shows the ProCurve Manager interface. The left sidebar displays a network tree with folders for Interconnect Devices, End-nodes, and Custom Groups. The main area shows a list of events with columns for Source, Severity, Status, Date, and Description. The selected event is expanded to show details:

Source	Severity	Status	Date	Description
NIAD	Minor	Blue	3/24/08 4...	Duplicate IP detected for IP 10.1.1.70, MAC1 00:18:71:b9:34:ce, MAC2 00:0e:7f:0f:ba:c9 Source IP = 10.1.1.70 Source MAC = Unknown Source TCP/UDP port = Unknown Destination
acct.procurveinc...	Minor	Blue	3/24/08 4...	IcmpHostUnreachable Protocol anomaly detected on srcIP:10.1.1.1[00:0e:7f:0f:ba:00] Source IP = 10.1.1.1 Source MAC = 00:0e:7f:0f:ba:00 Source TCP/UDP port = 3 Destination IP =
core.procurveinc...	Minor	Blue	3/24/08 4...	IpBothAddressesIdentical Protocol anomaly detected on srcIP:10.1.1.3[00:0f:1f:2a:f7:90] Source IP = 10.1.1.3 Source MAC = 00:0f:1f:2a:f7:90 Source TCP/UDP port = 6 Destination IP =

Event Details

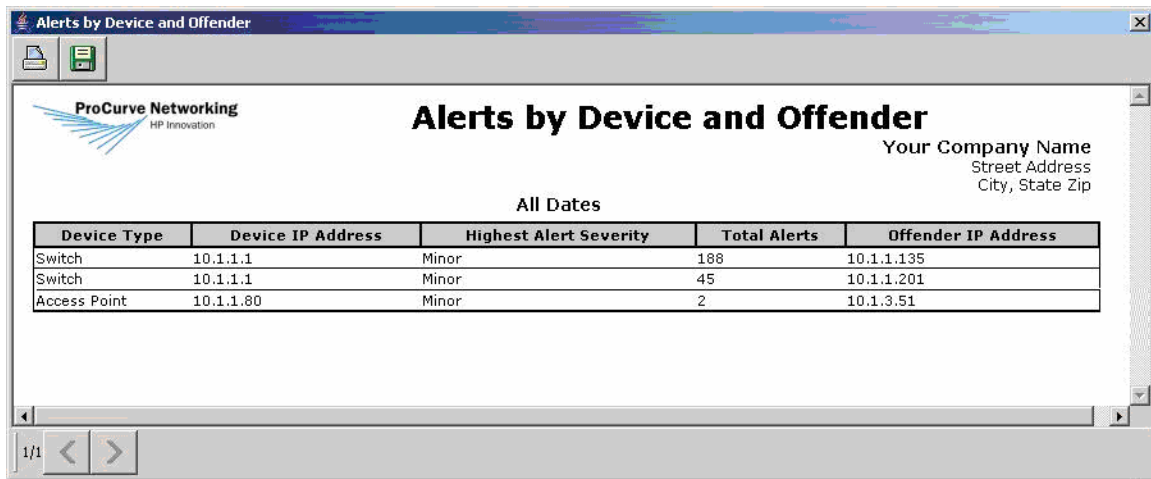
Event type: PCM Event
Received from: 10.1.1.1
Date received: Mon Mar 24 16:33:45 MDT 2008
Date acknowledged: Event has not been acknowledged.
Severity: Minor
IpBothAddressesIdentical Protocol anomaly detected on srcIP:10.1.1.3[00:0f:1f:2a:f7:90]
Source IP = 10.1.1.3
Source MAC = 00:0f:1f:2a:f7:90
Source TCP/UDP port = 6
Event Description: Destination IP = 10.1.1.3

Total rows: 1057

Based on the alerts that you see, what is the probable threat?

- A. worm
- B. Denial of Service (DoS) attack
- C. a covert channel tunneling data
- D. unauthorized network reconnaissance

2. Click the Exhibit button.



Alerts by Device and Offender

Your Company Name
Street Address
City, State Zip

All Dates

Device Type	Device IP Address	Highest Alert Severity	Total Alerts	Offender IP Address
Switch	10.1.1.1	Minor	188	10.1.1.135
Switch	10.1.1.1	Minor	45	10.1.1.201
Access Point	10.1.1.80	Minor	2	10.1.3.51

You run PCM+ with ProCurve NIM and IDM. In the report shown in the exhibit, you see that an offender has triggered 188 alerts. How do you find the offender's username?

- A. Go to the Security Activity -> Offender tab for the device shown in the Offender IP column. Double-click the offender's name.
- B. Go to the Security Activity -> Offender tab for the device shown in the Device IP column. Double-click the offender's name.
- C. Go to the Security Activity -> Offender tab for the device shown in the Device IP column. Double-click the offender's alert count.
- D. Go to the Security Activity -> Offender tab for the device shown in the Offender IP column. Double-click the offender's alert count.

3. What is a goal for your second time through the network immunity lifecycle?

- A. Refine policies.
- B. Plan and create policies.
- C. Finalize NBAD sensitivities.
- D. Exclude non-ProCurve routers from NBAD.

4. Which event type relies on the SNMP read-write community being correctly configured on ProCurve infrastructure devices?
- A. NBAD events
 - B. Scheduled events
 - C. Virus Throttle events
 - D. External security events
5. When should you examine security activity and plan policies?
- A. 24 hours after you install ProCurve NIM
 - B. one week after you install ProCurve NIM
 - C. as soon as you install ProCurve NIM and one week later
 - D. a day or so after you install ProCurve NIM and periodically

Answers

1. B
2. B
3. B
4. A
5. D

Conclusion

HP wishes you success in the HP Certified Professional Program and in passing the exam for which you are preparing.