

Overview

Models

ProCurve Network Access Controller 800

J9065A

Introduction

The ProCurve Network Access Controller 800 combines a RADIUS-based authentication server and the ability to validate the integrity of the systems connecting to the network, allowing network administrators to secure the network from unauthorized users and systems that pose a threat to the network resources.

Features and benefits

Management

- **Centralized endpoint policy management:** endpoint testing policies are centrally managed by a single management server and shared by up to 10 enforcement servers
- **Administration console:** a Web-based console provides an easy-to-use interface for configuring endpoint policies and enforcement clusters as well as a dashboard-style interface for viewing the status of endpoint integrity testing
- **Default testing policies:** default testing policies provide a great starting point for endpoint testing and can be easily utilized as the basis for custom testing policies
- **Network management server integration:** the ProCurve Network Access Controller 800 management server is discovered and monitored by the ProCurve Manager (PCM) management platform to enable unified device and security management; the Web-based administration console of the ProCurve NAC 800 is integrated into the PCM management display for a cohesive management experience

Performance

- **Efficient endpoint testing:** typical endpoint testing can be completed in less than 10 seconds, avoiding lengthy wait times as endpoints are connected to the network
- **Support for up to 30,000 concurrent endpoints in one management domain:** each enforcement server can support up to 3,000 endpoints, and one management server can control up to 10 enforcement servers

Resiliency and high availability

- **Enforcement server resiliency and redundancy:** enable high network availability for mission-critical LAN deployments; enforcement servers continue to provide authentication and endpoint testing services in the absence of a management server and can be configured in clusters to provide redundancy and load-balancing for endpoint testing

Security

- **Built-in RADIUS server:** can perform authentication services or act as a proxy server for a remote RADIUS authentication service
- **Supports standard-based or a local authentication directory:** can integrate with existing Active Directory or standard LDAP directory services or can host a local authentication directory for smaller environments
- **Endpoint integrity assessment—enables both pre-authentication and post-authentication testing of network-attached endpoints; includes an extensive set of built-in endpoint tests and is extensible to test for any prohibited or required software:**
 - **Operating system:** versions, service pack levels, and hot fixes
 - **Security settings:** firewall, auto-update, and browser security settings

Overview

- **Security software:** anti-virus, anti-spyware, firewalls
- **Malware:** spyware, worms, viruses, trojans
- **Applications:** peer-to-peer and instant messaging software
- **Flexible enforcement modes—offer multiple enforcement modes that can be used together and centrally managed by a single management server to share endpoint policies and licenses:**
 - **RADIUS:** integrates with RADIUS authentication to allow access only to authorized users and devices; uses RADIUS authorization capabilities to isolate endpoints for testing prior to providing complete network access and isolation of noncompliant endpoints
 - **DHCP:** integrates with DHCP servers to isolate and test endpoints before they are allowed to access production networks and interact with other network clients and resources
 - **Inline:** actively monitors a link for new endpoints and tests them before they are allowed to access the network; enables testing of remote endpoints connecting through a VPN concentrator
- **Flexible testing methods—enables endpoint testing that meets the broad needs of most businesses, including solutions for both managed and unmanaged endpoints:**
 - **Agent-based:** a permanent agent can be installed on endpoints to evaluate endpoint integrity status; it is the most efficient mode for managed endpoints that will continually connect to the network
 - **Transient agent:** an agent is temporarily downloaded to the endpoint to evaluate endpoint integrity, and then it enables unmanaged endpoints to be tested without the need to have an agent preloaded and remain on the endpoint
 - **Agentless:** uses administrative credentials for an endpoint along with native communications protocols to evaluate the endpoint integrity status; enables endpoints that are part of a managed domain or have known administrative credentials to be tested without ever loading an agent
- **Endpoint quarantine:** policy-based enforcement allows for isolation of noncompliant endpoints
- **Configurable remediation feedback:** provides administrator-customized feedback to users on how they can remediate their systems and be allowed full network access
- **Integration with Microsoft SMS:** Endpoints that fail testing and are also managed by a Microsoft Systems Management Server (SMS) agent will be prompted to contact the SMS for updates and will be retested once updates have been applied

Policy management

- **Policy-based network access rights:** integrate with ProCurve Identity Driven Manager (IDM) and network devices to apply centrally managed network access policies to be enforced at the edge of the network where users and devices attach; allow network administrators to easily create and maintain robust access policies, including secure guest access to appropriate network services, without risk to the network

Product Architecture

- **The ProCurve Network Access Controller 800 can be configured to take on different roles in a secure network access solution:**
 - **Management server:** a centralized server that manages and monitors multiple enforcement servers, including the endpoint integrity policies and centralized logging of endpoint authentication and test results, availability, and status
 - **Enforcement server:** provides RADIUS-based authentication of endpoints, along with testing of endpoints to evaluate compliance with endpoint integrity policies, policy-based isolation of noncompliant endpoints, and customized user feedback on how to remediate issues
 - **Combination server:** a single-server solution that combines the management server and enforcement server roles into a single appliance solution. A combination server only manages the enforcement server that is running in the combination server. A combination server can also be used in conjunction with ProCurve Identity Driven Manager (IDM) to provide RADIUS-based authentication and the IDM adaptive networking capabilities without endpoint integrity testing
 - **NOTE:** endpoint integrity testing is a capability that requires the additional purchase of ProCurve NAC Endpoint Integrity Agent licenses (see Accessories) and an initial Implementation Startup Service provided by a ProCurve-certified service provider or purchased through ProCurve (see Services).

Overview

Services

3-year, parts only, global next-day advance exchange	UH199E
3-year, 4-hour onsite, 13x5 coverage for hardware	UH196E
3-year, 4-hour onsite, 24x7 coverage for hardware	UH197E
3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support	UH198E
Installation with minimum configuration, system-based pricing	U4826E
1 Year Post Warranty Next Bus. Day Exchange	UH200PE
1 Year Post Warranty 4 hour response 13x5 Onsite Support	UH201PE
1 Year Post Warranty 4 hour response 24x7 Onsite HW Support	UH202PE
1 Year Post Warranty HW and SW 24x7 Phone Support	UH203PE
Startup of the NAC 800 with EI - DHCP and Inline	J9083A
Startup of the NAC 800 with EI - 802.1x	J9084A

Technical Specifications

ProCurve Network Access Controller 800 (J9065A)	Ports	2 RJ-45 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T); Duplex: 10Base-T/100Base-TX: half or full; 1000Base-T: full only 1 serial console port
Physical Characteristics	Dimensions	15.38(d) x 17.32(w) x 1.75(h) in. (39.07 x 43.99 x 4.45 cm) (1U height)
	Weight	13.45 lb. (6.1 kg)
Memory and Processor	Processor	Intel Core 2 Duo @ 2130 MHz, 2 GB DDR2 SDRAM
Mounting		Mounts in an EIA-standard 19 in. telco rack or equipment cabinet (hardware included); horizontal surface mounting only
Environment	Operating temperature	41°F to 104°F (5°C to 40°C)
	Operating relative humidity	15% to 80%, non-condensing
	Non-operating/storage temperature	-40°F to 149°F (-40°C to 65°C)
Electrical Characteristics	Max heat dissipation	434 BTU/hr (457.87 kJ/hr)
	Voltage	100-127 / 200-240 VAC
	Current	2 / 1 A
	Power consumption	127 W
	Frequency	50 / 60 Hz
Safety		CAN/CSA 22.2 No. 60950-1; IEC 60950-1; EN 60950-1
Emissions		FCC part 15 Class A; EN 55022 Class A
Immunity	EN	EN 55024, CISPR 24
	Harmonics	EN 61000-3-2, IEC 61000-3-2
	Flicker	EN 61000-3-3, IEC 61000-3-3
Management		ProCurve Manager Plus; Web browser
Notes		Endpoint Support for ProCurve NAC EI Agents <ul style="list-style-type: none">• Windows Vista, Windows XP, Windows Server 2003, Windows 2000, Windows NT, and Mac OS X Related Services• J9063A - ProCurve NAC Endpoint Integrity Implementation Startup Service (Inline and DHCP)• J9064A - ProCurve NAC Endpoint Integrity Implementation Startup Service (IEEE 802.1x)

Technical Specifications

Accessories	ProCurve NAC Endpoint Integrity Agent License for 100 clients	J9066A
	ProCurve NAC Endpoint Integrity Agent License for 250 clients	J9067A
	ProCurve NAC Endpoint Integrity Agent License for 1,000 clients	J9068A
	ProCurve NAC Endpoint Integrity Agent License for 5,000 clients	J9069A
	ProCurve NAC Endpoint Integrity Agent 1 year Maintenance License for 100 clients	J9070A
	ProCurve NAC Endpoint Integrity Agent 1 year Maintenance License for 250 clients	J9071A
	ProCurve NAC Endpoint Integrity Agent 1 year Maintenance License for 1,000 clients	J9072A
	ProCurve NAC Endpoint Integrity Agent 1 year Maintenance License for 5,000 clients	J9073A

© 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services.

Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

To learn more, visit www.procurve.com
Information is subject to change without notice.