

ProCurve Security Solution

Network Access Control

ProCurve's comprehensive network access control solution fortifies network security by authenticating users and devices before they are allowed onto the network.

Introduction to network access control

Network access control (NAC) is an industry-standard term used to describe methods and tools to selectively allow only authorized users, devices, and applications to gain access to networked resources. NAC is considered an important first line of network security.

Organizations face numerous challenges that drive the need for a comprehensive access control solution. These challenges include greater reliance on networked resources by employees; an increase in the number of employees who want mobile and remote access to the corporate network; growing requests for at least partial network access by partners, contractors, temporary workers, and guests; and increased need to comply with internal and external regulations.

ProCurve's network access control solution is part of the broader ProCurve ProActive Defense solution, a comprehensive network security strategy that simultaneously combines access security (proactive, offensive security) with network immunity (responsive, defensive security), within a trusted network infrastructure.

In ProCurve's network access control solution, access is controlled at the first point of attachment to the network—for example, LAN, WLAN, remote VPN—as directed by a policy.

By limiting who can gain access to specific information and resources on the network, at what time day access is available, and what devices can be used and from what locations, network administrators can fortify their network security while improving network performance and availability, as well as improving the network's ability to function as a strategic business asset.

Personalizing the network experience

With the right network access control solution, network administrators can alter individual users' entire network experience based on their role in the organization, the time of day they're connecting, their physical location, or the type of device they are using.

Employees can be granted easy access to the resources they need to be most productive, but not to resources outside of their domain of expertise. They might be assigned different connection speeds based on the time of day or night they're connecting, or have their access prioritized according to who else needs a higher-bandwidth connection.

When users access the corporate network remotely using laptops or other mobile devices, those devices can be given more careful scrutiny before being allowed access, to make sure they have not been compromised by a virus or other malware.

While network access control is typically considered a pre-admission network management tool—that is, controlling who gains access to the network in the first place—ProCurve's network access control solution also acts in a post-admission capacity by controlling user activities and network behavior after admission has already been granted.

ProCurve's network access control benefits

Some of the network security benefits derived from implementing ProCurve's network access control solution include that it:

- Secures the network from unauthorized users and systems that pose a threat to network data or resources

- Provides highly customizable role-based access to network resources for employees, contingent workers, vendors, suppliers, and customers
- Actively prevents security breaches and protects the network before a breach occurs, from both external and internal threats
- Prevents denial-of-service (DoS) attacks
- Dynamically controls which users and devices can gain access to the network, as well as what those users are able to do once they're granted access
- Protects the integrity and confidentiality of an organization's private or sensitive data
- Prevents "rogue" devices from gaining access to the network
- Prevents wireless devices from exploiting the network
- Works seamlessly across both wired and wireless networks
- Through post-admission network access control, helps protect assets after a user or device connects to the network
- Works with Microsoft® Network Access Protection (NAP) to help prevent security breaches
- Delivers superior return on IT investment through its scalability and industry standards-based approach

Highlights of ProCurve's network access control solution

Enhanced for the network edge

ProCurve's network access control solution offers unparalleled flexibility and advanced functionality specifically designed for the edge of the network, which is where users and devices connect.

Comprehensive network access control

As part of the ProActive Defense strategy, ProCurve's network access control solution is woven into the comprehensive network security framework, working seamlessly with defensive security approaches within a trusted network infrastructure.

Security problems prevented before they occur

As the "proactive" aspect of ProCurve ProActive Defense, ProCurve's network access control solution is designed to identify specific users and to enable the integrity of devices attempting to connect to an organization's network.

Better use of network resources

Even after network access has been granted, ProCurve's network access control solution continues to deliver benefits, improving and personalizing the network experience for the sake of users and the organization itself.

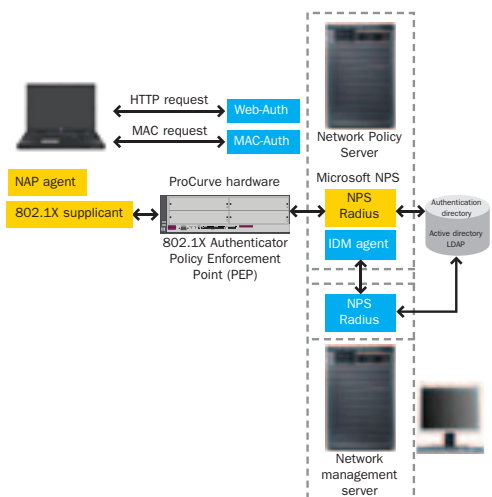
Unified access control across all network types

Because ProCurve's network access control solution offers unified access control across both wired and wireless networks, IT managers no longer need two separate management systems to control network access.

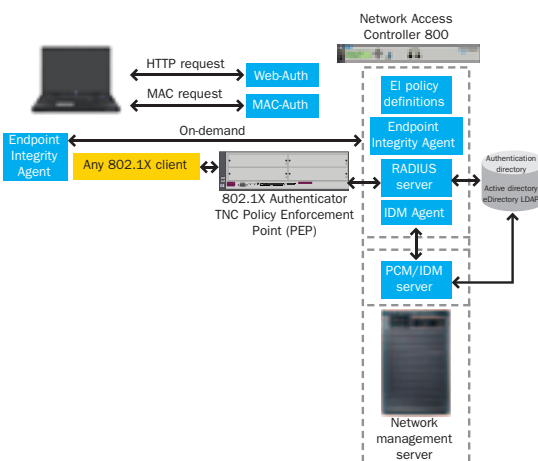
Flexible wireless guest access

ProCurve's network access control solution lets organizations deliver customizable guest services through a guest portal, making it easy for receptionists to securely provision guests, vendors, and suppliers without having to involve IT resources.

ProCurve network access control solution with IDM and Microsoft NAP



ProCurve network access control solution with IDM and NAC 800



Business continuity and competitiveness

By controlling access to the network, ProCurve's network access control solution helps the network's resources. And because they have easy access to the full array of network data and resources they are authorized to use, workers become more productive and thereby boost their organizations' competitiveness. In addition, ProCurve's network access control solution enables network administrators to fine-tune network usage to improve network performance at the same time they are fortifying security.

Flexibility and interoperability

The ProCurve network access control solution interoperates with and complements existing environments, such as Microsoft NAP, so that organizations can choose the products and services that best achieve their business goals. The ProCurve network access control solution is scalable and based on industry standards, thus giving organizations great flexibility in how they implement their network security solutions.

Solution features

Advanced, trusted security

- Grants appropriate access at the point of entry into the network
- Enables security across a wide range of complex applications and functionalities
- Provides advanced edge-centric security features such as access control lists (ACLs)
- Protects business assets while making them easily available to authorized users

Flexible access control options

- Controls access based on multiple variables, including user identity, device type, time of day, location, and endpoint configuration and overall health
- Offers Web-based authentication, to authenticate non-IEEE 802.1X-capable clients using a standard Web interface
- Complements the Microsoft NAP architecture with effective network access security technologies that are built into ProCurve switches and access points

Unified wired and wireless management

- Works seamlessly across all types of networks, using a common back-end authentication infrastructure for both wired and wireless networks
- Simplifies network management
- Reduces costs compared to maintaining and operating multiple, separate access security solutions

Comprehensive access control

- Allows network administrators to control which users have access to which resources on the network
- Dynamically configures security and performance settings based on user, device, location, time, and client system state

- Enables administrators to centrally define and apply policy-based network access rights that allow the network to automatically adapt to the needs of users and devices as they connect
- Protects the internal network edge as well as the external edges
- Integrates naturally with the other aspects of ProCurve ProActive Defense: network immunity and trusted network infrastructure

Endpoint integrity

- Includes a RADIUS-based authentication server as well as the ability to validate the integrity of the systems connecting to the network
- Enables network administrators to secure the network from unauthorized users and systems that pose a threat to network resources

Network visibility and control

- Enables IT managers to instantly know where guest devices are accessing the network
- Allows enforcement of access limits based on time of day, duration, and location of access
- Permits roaming of mobile clients while strictly enforcing access policies

Application control

- Uses a packet-filtering firewall built into ProCurve intelligent switches to filter incoming traffic based on IP address and ports
- Prevents unwanted and unauthorized application traffic from entering the network

Products to implement the ProCurve network access control solution

ProCurve weaves its network access control solution throughout its network infrastructure as well as offers specific products, including:

- **ProCurve ProVision™ ASIC:** Built into ProCurve switches, including the 5400zl series, 8212zl core switch, 3500yl series, and 6200yl series. This advanced network processor chip provides embedded security features such as network access control and network immunity capabilities.
- **ProCurve Wireless Edge Services Module with radio ports and access points:** Lets organizations provide Internet-only access or highly controlled and sophisticated guest access control to vendors, partners, and contractors. Features include time-of-day, location, and duration access control.

- **ProCurve Network Access Controller (NAC) 800:**
Enables the ProCurve network access control solution to evaluate the integrity of endpoints before they are allowed to access the organization's network. In addition, the Network Access Controller 800 provides a RADIUS authentication capability that integrates with the ProCurve command-from-the-center management platform. The ProCurve Network Access Controller 800:
 - Denies or isolates infected or harmful devices so that they cannot attack other network systems
 - Reduces costly network and system downtime
 - Continues to test endpoints while they remain connected to the network
 - Is designed with multiple enforcement modes:
 - IEEE 802.1X enforcement
 - In-line enforcement
 - Dynamic Host Configuration Protocol (DHCP) enforcement
 - Works with ProCurve's proven Identity Driven Manager (IDM) technology
- **ProCurve Identity Driven Manager (IDM):**
A plug-in to ProCurve Manager Plus that helps enhance network security and improve productivity by enabling automatic configuration of the network edge through security and management policies defined on a centrally administered server. ProCurve IDM allows network administrators to dynamically apply security and performance settings to network infrastructure devices based on user, device, location, time, and other variables
 - Provides the centralized policy management interface for defining network access rights and monitoring network access
 - Integrates with standard RADIUS authentication services and user directories (LDAP and Active Directory) to authenticate user and/or devices connecting to the network
 - Provides each network connection with unique and appropriate network access
 - Allows security and performance settings to be enforced as close to the endpoint as possible

- Identifies the appropriate level of access based on information about the users and communities
- Enables any switch and port to act uniquely for each individual user
- Adapts appropriately to the needs of each user, as defined by corporate policy
- **ProCurve Manager Plus (PCM+):** Network management software that operates across both wired and wireless networks, enabling unified, easy management of network security from an offensive as well as a defensive perspective.
- **ProCurve Mobility Manager:** Provides visibility into wireless client activity and locates network-attached guest devices.
- **ProCurve Network Immunity Manager (NIM):** A plug-in to ProCurve Manager Plus that detects and automatically responds to threats, such as virus and worm attacks, inside the network. It monitors devices across the network for internal network attacks and allows administrators to set detection and response security policies.
- **ProCurve Network Access Controller Endpoint Integrity Implementation Startup Service:** Provides expertise to help your organization implement your ProCurve Network Access Controller with endpoint integrity.

Summary

ProCurve's network access control solution can be easily deployed and managed using the ProCurve command-from-the-center management approach, and it is especially effective when used in conjunction with other ProCurve ProActive Defense solutions. The ProCurve network access control solution is crucial for the proactive, or offensive, aspects of ProActive Defense that actively prevent security breaches and protect the network before a breach occurs. The solution then empowers network administrators to improve network security and performance by controlling individual users' access to the corporate network's information and resources.

For more information

To learn more about ProCurve Networking, please visit www.procurve.com/security

© 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.

Microsoft is a U.S. registered trademark of Microsoft Corporation.

4AA1-8679ENW, April 2008

