

ProCurve Security Solution

ProActive Defense

ProCurve's ProActive Defense security strategy delivers a trusted network infrastructure that is immune to threats, controllable for appropriate use, and able to protect data and integrity for all users.

Introduction to network security

A network today is a business-critical strategic asset that directly affects an organization's competitiveness in rapidly changing business environments. Everyone understands the importance of protecting the network from potentially devastating breaches. How to implement effective network security, however, is less obvious.

Consider that in 2007, the number of publicly reported data breaches in the U.S. rose by more than 40 percent compared to 2006.¹ And according to the 2007 CSI Computer Crime and Security Survey, more than half of the organizations surveyed (U.S. corporations, government agencies, financial institutions, medical institutions, and universities) experienced computer security incidents during the previous year.

In addition to occurring more frequently, network security breaches also translate into increasing financial costs. The CSI survey's participants reported losses averaging US\$345,000 per respondent—more than double the amount reported one year earlier.

Modern network security has evolved from erecting a firewall and perhaps some basic virus protection to the need for a comprehensive, multi-layered approach. At the same time, however, network security measures must not hinder the manageability of the network or the ability of users to access the network information and resources they need to perform optimally.

ProActive Defense: combining offense and defense, simultaneously

ProCurve ProActive Defense is a comprehensive security vision and strategy, translated into an evolving range of security solutions. ProActive Defense

automates protection, detection, and response within a trusted network infrastructure.

ProActive Defense is unique in its simultaneous combination of both offensive and defensive approaches to protecting IT assets.

ProCurve ProActive Defense has three foundational principles:

- **Trusted network infrastructure.** A trusted network infrastructure is a platform for policy automation—that is, the process of automatically protecting, detecting, and responding to threats. It includes the protection of network components, the prevention of unauthorized security policy overrides, and privacy measures to ensure the integrity and confidentiality of sensitive data.
- **Proactive security = access control.** This “offensive” security proactively prevents security breaches by controlling which users have access to systems and how they connect in both a wired and wireless network. Proactive security is designed to stop problems before they occur by helping to ensure that all network users are always authenticated and that all devices adhere to endpoint security policies.
- **Defensive security = network immunity.** Defensive security is about detecting and responding appropriately to network threats, thereby defending the network from virus, worm, trojan horse, and other malware attacks. Defensive security monitors network behavior—both intentional and accidental actions, originating from the outside or inside of an organization—and applies security information intelligence to protect the integrity, privacy, and performance of the network and the data and resources running on it.

¹ Source: statistics compiled by the Identity Theft Resource Center (ITRC), a consumer rights advocacy group.

The underlying, holistic foundation of ProActive Defense

It is important to recognize that effective network security is a process, not a specific product or solution. The dynamic nature of network operations means that security must be automated, so that the network itself can react to and repel threats.

The ProCurve Networking Adaptive EDGE Architecture™ (AEA) establishes the necessary foundation for security and is based on the principles of command from the center with control to the edge. The AEA's *command from the center*—the ability for ProCurve management tools to set security policies and report alerts and information about the security of the network—provides unified access to critical network resources based on policies enforced at the individual user level.

The AEA's *control to the edge* of the network means that decisions about security happen automatically, at the point where users and devices connect. This approach leads directly to more efficient, less complex, and more flexible network and security management.

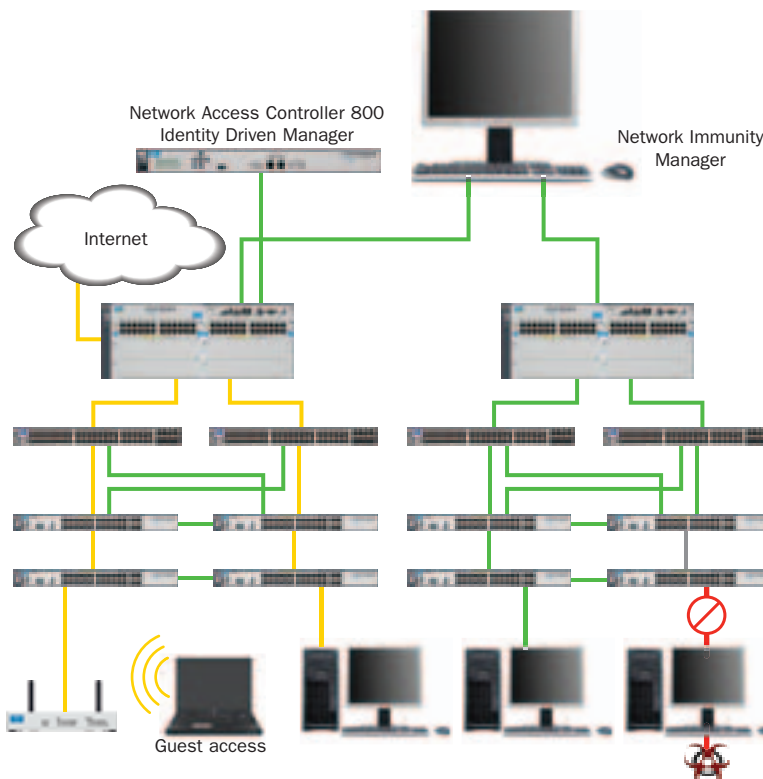
Because the ProActive Defense strategy arises from this AEA foundation, it is able to provide the comprehensive, multi-layered network security approach demanded by organizations today.

ProCurve ProActive Defense benefits

The advantages of adopting a ProCurve ProActive Defense strategy include that it:

- Delivers a trusted network infrastructure that is immune to threats, controllable for appropriate use, and able to protect data and integrity for all users
- Provides a multi-layered and effective approach to network security that combines both offensive and defensive security, simultaneously
- Integrates security and centralized management within a unified wired and wireless network environment
- Protects an organization's important and sensitive information and resources from misuse
- Prevents network security breaches by controlling user and device access to the network
- When breaches do occur, identifies the source (i.e., specific switch port) and mitigates the attack at the origination point
- Correlates network threat events and dynamically responds to attacks, thus reducing their damage
- Responds automatically to defend the network against attacks and unwanted network traffic
- Strengthens and simplifies demonstration of compliance for both internal and external requirements

ProCurve ProActive Defense



- Enables network managers to turn security intelligence into actionable items
- Interoperates with multivendor networking hardware and software products because it is based on industry standards
- Accepts security attack alerts from third-party security devices—such as intrusion detection/intrusion prevention system (IDS/IPS) and unified threat management (UTM) appliances—to further defend against threats

Highlights of ProCurve's ProActive Defense solution

Comprehensive, multi-layered protection of the entire network

ProActive Defense is woven into the fabric of the network itself, and the simultaneous combination of offensive and defensive security approaches provides coverage against the full range of security threats a network might face. The ProCurve ProActive Defense principles and tools provide overall network availability and robustness.

Unified security management across wired and wireless networks

ProActive Defense provides a single, comprehensive strategy that works—and can be managed—across all types of networks, including both wired and wireless, with a “single pane of glass” approach. Security policies are dynamically enforced at the edge of the network, where users, applications, and devices connect.

Optimal productivity

ProActive Defense solutions give an organization the best possible chance to avoid network outages or degradation in performance. At the same time, ProActive Defense maintains easy user access to the full array of network data and resources they are authorized to use—so that they can improve their productivity.

Business continuity and competitiveness

ProCurve ProActive Defense helps an organization's mission-critical networks remain up and running and available to users. In addition, the manageability of the ProActive Defense solutions means that an organization's IT staff can spend less time actively overseeing the network operations and more time harnessing the network to achieve business goals and improve competitiveness.

Regulatory compliance

ProCurve enables the centralized establishment of security policies that are enforced automatically throughout the network, thereby making it easier to comply—and demonstrate compliance—with regulations set forth by government agencies, supply-chain partners, and internal auditors. For example, ProCurve's products and technologies generate reports

that help monitor the execution of security policies and assist in the control of the IT infrastructure as part of a larger compliance program.

Flexibility

The various aspects of ProActive Defense can be implemented in phases and scaled as businesses grow and their needs expand. Additionally, ProCurve's dedication to defining and supporting industry standards makes its security solutions interoperable with a wide range of hardware, software, and tools from other standards-compliant networking and network security products.

Solution features

Trusted network infrastructure

ProCurve builds ProActive Defense capabilities into its switches. Most notably, the ProCurve ProVision™ ASIC network processor chip includes a range of embedded security features, including enforcement of both access control and defensive policies.

ProCurve Manager Plus (PCM+) network management software operates across both wired and wireless networks, enabling unified, easy management of network security from an offensive as well as a defensive perspective.

Access control

ProCurve's powerful network access control solution delivers unified wired and wireless access control.

ProCurve offers network access control (NAC) hardware that provides endpoint integrity, with a RADIUS-based authentication server as well as the ability to validate the integrity of the systems connecting to the network. As a result, network administrators can secure the network from unauthorized users and systems that pose a threat to network resources.

ProCurve Identity Driven Manager (IDM) software lets administrators control which users have access to which resources on the network. IDM dynamically configures security and performance settings based on user, device, location, time, and client system state. Network administrators can 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—thereby enforcing network security while providing appropriate access to authorized users and devices.

Network immunity

ProCurve Network Immunity Manager software 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. It leverages security and traffic-monitoring features built into the ProVision ASIC.

In ProCurve switches based on the ProVision ASIC, the following network immunity capabilities are built in:

- Virus throttling technology, an algorithm that rapidly detects and quarantines a virus or worm, preventing its ability to spread and disarming its ability to harm the network
- sFlow® industry-standard technology, designed to monitor high-speed switched networks and defend against security threats such as malicious activities or zero-day attack behaviors
- Network Behavior Anomaly Detection (NBAD), which detects attacks
- IDS/IPS capabilities, including:
 - Internet Control Message Protocol (ICMP) throttling
 - Dynamic Host Configuration Protocol (DHCP) protection
 - Dynamic Address Resolution Protocol (ARP) protection
 - Bridge Protocol Data Unit (BPDU) port protection
 - Spanning Tree root protection
 - Switch CPU protection

Products to implement the ProCurve ProActive Defense strategy

ProCurve ProActive Defense solutions are integrated throughout ProCurve's network infrastructure as well as embodied by specific offerings.

Trusted network infrastructure

- ProCurve ProVision ASIC, built into ProCurve switches including the 5400zl series, 8212zl core switch, 3500yl series, and 6200yl series
- ProCurve Manager Plus (PCM+) 2.x network management software

Access control

- ProCurve Network Access Controller (NAC) 800
- ProCurve Identity Driven Manager (IDM) 2.x, a plug-in to PCM+

Network immunity

- ProCurve Network Immunity Manager (NIM), a plug-in to PCM+

Summary

Networks have become mission-critical, so organizations cannot afford to risk the security of their network operations, resources, or data. ProCurve's ProActive Defense is the industry's first holistic, comprehensive, multi-layered network security strategy that spans both offensive and defensive security measures simultaneously, within a trusted network infrastructure.

Through its sophisticated integration of a secure infrastructure, access control and network immunity, ProActive Defense prevents security breaches before they occur, automatically detects external and internal security threats, protects the privacy of data, and responds automatically and appropriately to any security breaches that still slip in. As a result, ProCurve ProActive Defense protects network data, resources, and integrity for all authorized users, so that an organization's network can fulfill its potential as a strategic business asset.

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.

4AA1-8676ENW, April 2008

