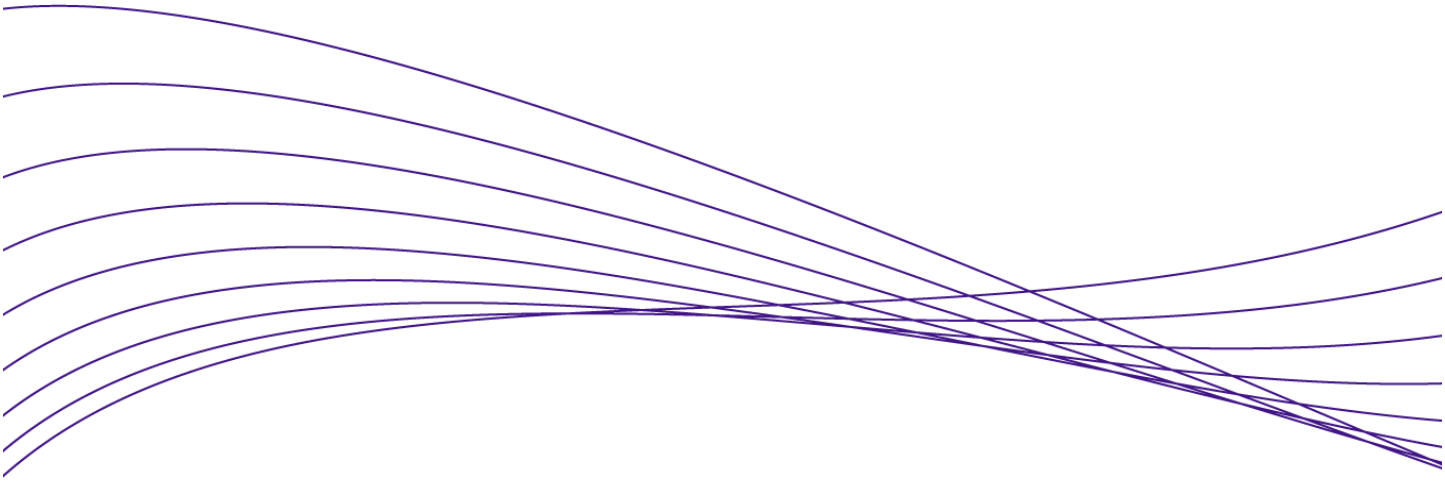
ProCurve Networking by HP

Comprehensive LAN Security: A Business Requirement



Introduction 2

The ProCurve ProActive Defense Strategy 3

Combining Security Offense and Defense 4

A Unified Platform for Network Management 5

How ProCurve Implements ProActive Defense 5

Embedded Security in the LAN Infrastructure 5

ProCurve Network Access Controller (NAC) 800 6

Endpoint Integrity Tests 6

RADIUS Authentication 6

ProCurve Identity Driven Manager (IDM) 7

ProCurve Network Immunity Manager (NIM) 7

Attack Detection 8

Response 8

Reporting 8

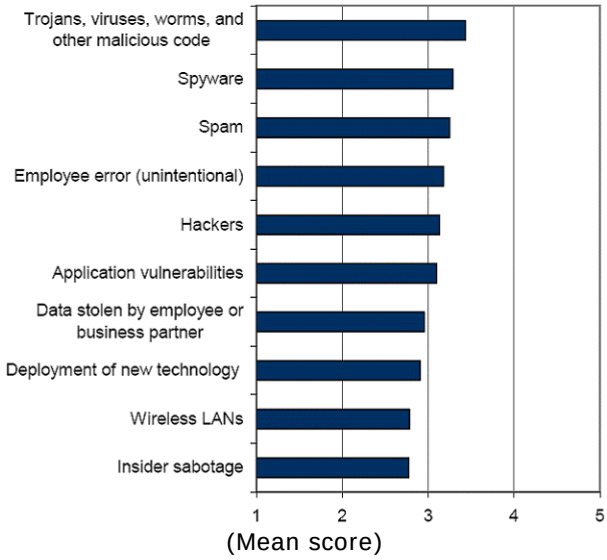
Case Example: Access Control and Integrity Checking 9

Summary 10

Introduction

Organizations rely on their networks for business-critical processes and information. In fact, local-area networks (LANs) are becoming crucial factors in an organization's ability to compete successfully in today's fast-paced, rapidly changing business climate. Unfortunately, these networks are under attack. Network threats have become more prevalent and creative in their design and often possess an increasing potential to disrupt and devastate core business operations.

Network threats including viruses, worms and Trojan horses and can include attacks introduced through internal sabotage as well as from outside forces. A 2006 survey by IDC (see Figure 1) illustrates the range of threats causing the most concern for enterprise security.



Note: Threat scores are based on a scale from 1 to 5, with 1=no threat and 5=significant threat.

Source: IDC *Security Survey*, 2006

Figure 1: Top 10 Threats to Enterprise Security

Organizations of all types and sizes – and their network administrators, IT managers and chief information officers (CIOs) – have good reason to be concerned about network security.

Statistics support the notion that network attacks are widespread and costly. According to the 2007 CSI Computer Crime and Security Survey (which included U.S. corporations, government agencies, financial institutions, medical institutions and universities), more than half of the organizations surveyed experienced computer security incidents during the previous year. Of those that responded, more than 25% reported 10 or more attacks. The reported losses averaged $345,000 per respondent – more than double the amount reported in the previous year.

While these public figures are significant, they represent only a fraction of the actual losses incurred from security breaches. In reality, reporting of security failures is often hampered by an organization's concerns about publicly revealing its vulnerabilities. As a result, it is difficult to measure actual market losses from network security failures nationwide.

While the severity and kinds of threats continue to multiply, corporate security experts are burdened with additional challenges, including the need to deploy wireless networks, support mobile workforces, provide shared network access and demonstrate compliance with government regulations.

In earlier times, erecting a firewall and implementing virus protection might have been considered a sufficient approach to network security. History, however, has shown otherwise. Organizations today need a network security approach that is comprehensive, multi-layered and manageable. ProCurve Networking by HP offers a comprehensive, holistic framework and specific tools for handling network security that puts an unprecedented level of control in the hands of network administrators.

This paper goes beyond a simple restatement of the problem of network security, proposing a viable solution: ProCurve's ProActive Defense strategy. The ProCurve ProActive Defense strategy delivers a cohesive network security approach, backed by products and services designed to give businesses the best possible chance to keep their networks up and running, and their crucial information and processes both safe and available.

The ProCurve ProActive Defense Strategy

The ProCurve ProActive Defense strategy recognizes an organization's need for a complete network security strategy – one that integrates with the organization's existing IT infrastructure, enforces internal controls, and reports security activities for auditing and forensics purposes. ProActive Defense returns control to businesses by allowing them to secure their networks, while at the same time enabling easy access by authorized users to the information and resources they need to perform their jobs.

Taking control of network security means that companies must:

- Control access to the network and enforce appropriate use.
- Prevent or eliminate viruses/worms and unwanted network traffic.
- Understand both the internal and external threats.
- Make sense out of the enormous amount of security intelligence available and turn it into actionable items.
- Understand and demonstrate regulatory compliance to internal auditors, government agencies and supply chain partners.

To enable companies to achieve these goals, security solutions should be:

- Based on a trusted IT infrastructure and a sound strategy that mitigates risk and returns control to the organization.
- Comprehensive.
- Easy to deploy and use.
- Standards-based, interoperable and reliable.

The ProCurve ProActive Defense strategy addresses these goals by delivering a trusted network infrastructure that is immune to threats, controllable for appropriate use and able to protect data and integrity for all users.

ProActive Defense is not a product or even a suite of products, but rather is a comprehensive, multi-layered strategy predicated on the vision of Adaptive Networks: networks that are adaptive to users, adaptive to applications and adaptive to organizations – all on a cohesive, flexible network infrastructure that is highly secure and available.

ProCurve's Adaptive Network vision is implemented through the ProCurve Adaptive EDGE Architecture™, which is based around two concepts: control to the edge and command from the center.

Control to the edge of the network means that intelligent security – the ability for the network to respond and react – is located at the edge of the network, where users and resources connect. With security enforced at the edge – as close to users, applications or devices as possible – administrators can better secure the network against threats, regardless of the source.

By moving important access and policy enforcement decisions to the edge of the network, ProCurve's Adaptive EDGE Architecture frees core resources to provide the high-bandwidth interconnect functions they are designed to perform. The result is not only better network security, but also better-performing, more flexible and scalable networks.

Command from the center gives network managers the ability to set policies based on business needs, driven by user identity, application and device type, and to report alerts and information about the security of the network. The Adaptive EDGE Architecture provides unified access to critical network resources based on policies enforced at the individual user level. As a result, organizations can more effectively protect secure data while making sure that authorized users gain access to the network resources they need to be most productive.

The cohesiveness and distributed intelligence of this architecture enables ProCurve to provide integrated security and centralized management within a unified wired and wireless network.

An important aspect of the Adaptive EDGE Architecture is that it is built on industry standards. ProCurve not only supports standards in its products, but also takes a leading role in the creation and adoption of networking industry standards – notably, the IEEE 802.1X standards for port-based network access control.

As a result of this standards leadership, ProCurve can ensure that its products interoperate with third-party solutions and provide long-lasting choice and flexibility for companies using these products. With standards-based security, companies avoid being locked into proprietary schemes that may or may not work with other equipment or under conditions that arise in the future.

Combining Security Offense and Defense

ProCurve's holistic approach – fortifying security from the core to the very edge of the network – helps to create a network that is immune to threats, with the ability to control access and usage, and to protect the data and integrity of its users.

The ProCurve ProActive Defense strategy combines pre-emptive, or offensive, techniques (e.g., comprehensive access control) with innovative defensive methods (e.g., automated threat detection and response), all within the context of a trusted network infrastructure (see Figure 2). Fortifying security for enterprises, without massive and costly replacement of network infrastructure, is a critical focus of ProCurve ProActive Defense.

ProCurve ProActive Defense is designed to:

- Prevent security breaches and protect the network *before* a breach occurs.
- Prevent unauthorized users from accessing or eavesdropping on the network.
- Prevent hosts and applications from being deployed on the network without authorization.
- Automatically detect external and internal security threats.
- Detect attacks during a security breach.
- Respond automatically and appropriately to a security breach.
- Correlate network threat events and dynamically respond to mitigate attacks.

Figure 2: ProActive Defense combines access control and network immunity, within a trusted network infrastructure.

A Unified Platform for Network Management

ProCurve's ProActive Defense tools allow the IT manager or network administrator to manage user access and mitigate security threats from a single console to:

- Define groups – communities of users who share common network access privileges – and then define rules, or policies, that grant the appropriate network access and other resources to members of each group.
- Set policies for detecting and responding to internal network security threats, leveraging technologies embedded into the switch.

Because it arises from this holistic Adaptive EDGE Architecture, ProCurve ProActive Defense delivers businesses a seamless, unified management approach to all its networks, whether wired or wireless.

How ProCurve Implements ProActive Defense

ProCurve's ProActive Defense strategy leverages both hardware and software technologies to deliver a comprehensive network security solution.

ProCurve ProActive Defense strategy also includes a number of ProCurve security-specific products – such as **ProCurve Network Access Controller (NAC) 800**, **ProCurve Identity Driven Manager (IDM)** and **ProCurve Network Immunity Manager (NIM)** – that harness the security capabilities embedded in ProCurve's LAN infrastructure. ProCurve IDM and ProCurve NIM are both software plug-ins to ProCurve Manager Plus (PCM+), comprehensive network management software that allows control of all aspects of network security, including advanced policy-based device and traffic management.

ProCurve's networking hardware and software work together to allow network administrators to strengthen their organizations' network security, providing a comprehensive and easy-to-manage network security solution.

Embedded Security in the LAN Infrastructure

Effective network security starts with a secure network infrastructure that is trusted, reliable, self-identifying and fully authenticated. At the same time, the infrastructure must remain plug-and-play and easy to manage. Security is not effective if it is too complex to implement or if it degrades the performance of the overall system.

For that reason, ProCurve's secure network infrastructure includes switches, access points and other hardware with built-in threat management and anomaly detection. In particular, the ProCurve-designed **ProVision™ ASIC** network processor chip includes embedded security features such as a packet filtering firewall, Virus Throttle technology, sFlow® technology and intrusion detection/intrusion prevention systems (IDS/IPS) capabilities. As a result, ProCurve switches based on ProVision ASICs (which currently include the ProCurve Switch 5400/3500/8200/6200 series products) provide unique insight and visibility into network traffic that other security vendors cannot provide.

The defensive security features that ProCurve built into its ProVision ASIC includes policy enforcement capabilities. The resiliency of the ProVision ASICs translates to switches that can operate even under malicious attack or network mis-configuration.

ProCurve intelligent switches can detect a spike in traffic, determine that an anomaly has occurred (for example, a dramatic increase in resources) and investigate the cause of the anomaly. ProCurve switches can thwart threats through security methods that are embedded in the switch's ASIC itself:

- A **packet filtering firewall**, available with ProCurve intelligent switches, filters incoming traffic based on IP addresses and ports, preventing unwanted (and unauthorized) application traffic from entering the network.
- **Virus Throttle** is an algorithm embedded within the ProVision ASIC that rapidly detects and quarantines a virus or worm, preventing its ability to spread and disarming its ability to harm the network. Virus Throttle is based on the detection of anomalous behavior of network traffic that differs from normal activity: the switch monitors 10 types of network traffic and sends a warning when it detects an anomaly that might be caused by malicious attacks.

- In addition to virus throttling, embedded **Intrusion Prevention** (**IPS**) capabilities include Internet Control Message Protocol (ICMP) Throttling, which defeats denial-of-service attacks by enabling any switch port to automatically restrict ICMP traffic; Dynamic Host Configuration Protocol (DHCP) protection; dynamic Address Resolution Protocol (ARP) protection; Bridge Protocol Data Unit (BPDU) port protection; and Spanning Tree root protection. Switch CPU Protection provides automatic protection against malicious network traffic trying to shut down the switch.
- The **sFlow** industry-standard technology is designed to monitor high-speed switched networks. sFlow support provides complete visibility into the use of networks, enabling defense against security threats such as malicious activities or zero-day attack behaviors.
- Administrators can monitor network activity on a switch using either **local or remote mirroring**. Local mirroring allows a network analyzer to monitor local switch traffic, whereas remote mirroring allows monitoring of remote switch traffic.
- ProCurve intelligent switches can restrict network access and work with ProCurve IDM to enforce security policies. Features include 802.1X, MAC/Web authentication, access control list (ACL) capabilities, port security, IP lockdown, MAC lockout and source port filtering.

Some of these capabilities also are embedded into ProCurve's unified wired and wireless infrastructure to provide pervasive security regardless of network type.

ProCurve Network Access Controller (NAC) 800

Today, a multitude of devices connect to the network, including laptops, IP phones, peripherals, PDAs and various wireless devices, as well as traditional desktop computers. It is essentially impossible for IT departments to mandate a specific operating environment for all devices that access the network.

The pre-emptive, proactive portion of a ProActive Defense strategy is primarily about access control: a comprehensive way of managing access to the network, capable of identifying and controlling access for all types of users. The goal of access control is to protect the network and its resources from harmful users and systems.

The ProCurve Network Access Controller (NAC) 800 secures the network against unauthorized users and non-compliant devices that may pose a threat to network resources. Based on business policies defined by the network administrator, the NAC 800 protects the network and individual users from harmful threats and enforces system software requirements.

Endpoint Integrity Tests

The primary role of the ProCurve NAC 800 is to evaluate the health of endpoints as they connect to the network. Verifying endpoints before they connect to the network allows infected or otherwise harmful systems to be denied access or isolated, so they cannot attack other network systems. This approach helps reduce costly network and system downtime. In addition, endpoints are tested while they remain connected to the network, providing an ongoing post-authentication health check.

The ProCurve NAC 800 provides a comprehensive set of tests to evaluate the current health of a system, as well as the appropriate configuration to protect itself from attacks by others. These tests include checks for:

- Operating system: versions, service packs, hotfixes, auto-update settings.
- Security software: antivirus, spyware, firewalls, peer-to-peer applications, allowed and prohibited programs and services.
- Security settings: for browsers and applications.
- Required and prohibited software: customizable by the administrator.
- Malicious software: checks for common spyware, worms, viruses and Trojans

RADIUS Authentication

The ProCurve NAC 800 also provides RADIUS-based authentication services to enable unified device and security management. RADIUS is a standards-based authentication service that is the foundation for almost all industry NAC solutions that use network infrastructure for

enforcement. This authentication service can be used with ProCurve IDM to provide the adaptive network access rights to network devices.

ProCurve Identity Driven Manager (IDM)

ProCurve Identity Driven Manager (IDM) provides the centralized policy management interface for defining network access rights and monitoring network access. A plug-in module to ProCurve Manager Plus (PCM+) network management software, ProCurve IDM help companies maximize network security and improve productivity, by enabling automatic and dynamic configuration of the network edge.

Security and management policies are defined in ProCurve IDM on a centrally administered server and can be applied to all ProCurve adaptive-edge devices, both wired and wireless. The result is a unified management infrastructure and a more secure, mobile and converged network.

ProCurve IDM also integrates with standard RADIUS authentication services and user directories (LDAP, Microsoft Active Directory or eDirectory) to authenticate users and/or devices connecting to the network, then adds a rich set of authorization capabilities on top of the basic authentication.

IDM allows a network administrator to define communities of users who share common network access privileges. Typically, these communities are defined by department (such as marketing) or by role (such as purchasing). Each community has a unique set of rules, based on business policy that indicates the level of network access users are entitled to when connected.

ProCurve IDM can provide unique access based on:

- Who the user is.
- What community(s) the user is associated to.
- Whether the user's device (PC, laptop, PDA, VoIP phone, etc.) is running the appropriate software required by the business.
- Where the user is located (switch/port).
- The time of access

IDM then determines the appropriate level of network access rights and can establish:

- Whether resources are made available/denied to that community(s).
- The performance attributes assigned to that community(s).

After the network administrator establishes the appropriate users, groups and access rules, the network is able to dynamically and automatically configure itself on a per-user, per-session basis. The network behaves appropriately according to the user's particular access rights, no matter where or when users access the network or what devices they use. ProCurve IDM ensures that switches and access points make the correct decisions and enforce policies at the perimeter of the network, where it is most effective.

ProCurve Network Immunity Manager (NIM)

ProCurve Network Immunity Manager (NIM), another plug-in module for PCM+, delivers pervasive intelligent network threat management, detection and response to help protect against threats such as virus attacks. It is part of the defensive capabilities of ProActive Defense.

ProCurve NIM leverages internal attack detection in conjunction with external network and security information to monitor the network for internal threats. It can pinpoint the source of security events and then leverage the network to mitigate those threats.

With ProCurve NIM, IT managers enjoy broad coverage against internal attacks and a rich set of mitigation and offender tracking capabilities. ProCurve NIM monitors access points and switch ports across the network for internal network threats, while allowing network administrators to set detection and response security policies. It turns access points and switch ports into security sensors, provides visibility into internal threat activity on the network and helps administrators maximize network availability.

ProCurve NIM assists IT administrators at various stages of threat management, ensures compliance of policies across their corporate networks and automatically mitigates threats at the point where the attack originates.

Attack Detection

There are two ways to deploy attack detection with ProCurve NIM: in standalone mode or in conjunction with third-party security devices.

In **standalone mode**, ProCurve switches send sampled traffic using sFlow technology to ProCurve NIM. ProCurve NIM then performs Network Behavior Anomaly Detection (NBAD) on the data, to detect and respond to internal threats in both wired and wireless networks. The NBAD system observes network traffic and builds a normal network usage profile. Unlike an anti-virus or IPS, the NBAD system doesn't rely on signature file matching, but instead detects behaviors symptomatic of viruses, worms or malicious users. When the current traffic flows deviate significantly from the established network profile, the NBAD system creates an alert to signal network administrators of a potential attack.

ProCurve NIM can accept virus alerts from ProCurve switches running Virus Throttle software, which detects IP Fan Out virus behavior. Internal threats detected by ProCurve NIM include zero-day and known viruses or worms, protocol anomalies, reconnaissance scans, IP spoofing and other network-based attacks, and anomalous packet sizes.

In **third-party mode**, ProCurve NIM can also accept alerts from select third-party security devices, such as IDS/IPS and unified threat management (UTM) appliances, that have already been deployed in strategic locations. This approach allows organizations to leverage existing security infrastructure by sending security alerts to ProCurve NIM.

ProCurve NIM can bring suspect traffic to a security device for inspection by leveraging ProCurve's Intelligent Remote Mirroring feature, embedded in ProVision-based switches. This capability allows the security device to be virtually deployed anywhere within the network on a moment's notice. The security device can then inspect the traffic and generate alerts that are subsequently consumed by ProCurve NIM for correlation, mitigation and logging purposes.

ProCurve NIM is compatible with a number of commonly used security appliances, such as those from Fortinet, SonicWALL and Cisco, to provide a unified network security architecture. The benefit to customers is a flexible, cost-effective approach designed to improve their overall network security. Support for the common industrial protocol (CIP) enables any kind of third-party IDS or UTM solution to be integrated into ProCurve NIM.

ProCurve collaborates with network security providers such as Fortinet and SonicWALL in the ProCurve Alliance, a formalized interoperability testing and certification program that provides comprehensive, pre-qualified solutions for resellers and customers worldwide. ProCurve is continually adding new strategic and solutions partners. For details, visit the ProCurve Alliance Web site (http://www.procurve.com/alliance).

Response

As security events occur, ProCurve Network Immunity Manager can be configured at multiple response levels, ranging from quietly recording events as they unfold to taking multiple active mitigation actions against a threat. ProCurve NIM can respond to attacks on a per-access-point or per-port basis, based on the policies set by the IT administrator. The spectrum of responses includes:

- Quarantine the attacker on a VLAN.
- Bandwidth rate-limit the port that originated the attack.
- Lock out the attacker's MAC address.
- Shut down the attacker's port.
- Mirror suspicious traffic to security device.
- Alert the IT administrator of the attack via email.

Reporting

The ProCurve Network Immunity Solution (PCM+ with the ProCurve NIM plug-in) can provide reports that include security policy reports and offender tracking reports for forensics. Through data mining, the Network Immunity Solution can generate network-based, offender-based and

alert-based tabular reports with various degrees of information granularity. Users can generate custom reports from the PCM database schema to assist with regulatory compliance.

Case Example: Access Control and Integrity Checking

To better understand how the ProCurve ProActive Defense strategy can work to safeguard a network, here is a simple case: a meeting between an employee and a supplier in a conference room.

Using their laptops, the employee and the supplier connect to the network, where they are authenticated by ProCurve Identity Driven Manager (IDM). ProCurve IDM works together with the ProCurve Network Access Controller (NAC) 800 to control which users have access to systems and how they connect across both wired and wireless networks. It doesn't matter whether they connect wirelessly or via the Ethernet; the same ProActive Defense security mechanisms are in place.

Once the employee and the supplier have been admitted to the network, the ProCurve NAC 800 and ProCurve IDM determine what resources each user can access, where they can go within the network and what boundaries will be imposed.

- The employee is granted access to the corporate intranet, along with other internal resources on the corporate server. While authenticating the employee, the ProCurve NAC 800 also verifies the employee's laptop applications and operating system (OS) patches are up to date and that the laptop has the latest updates to security software (personal firewall, virus protection, etc.).
- The supplier's access is based on the organization's predetermined policy for guest users. In this case, the supplier is granted Internet access with a maximum of 2 Mbps and a limited set of network resources.

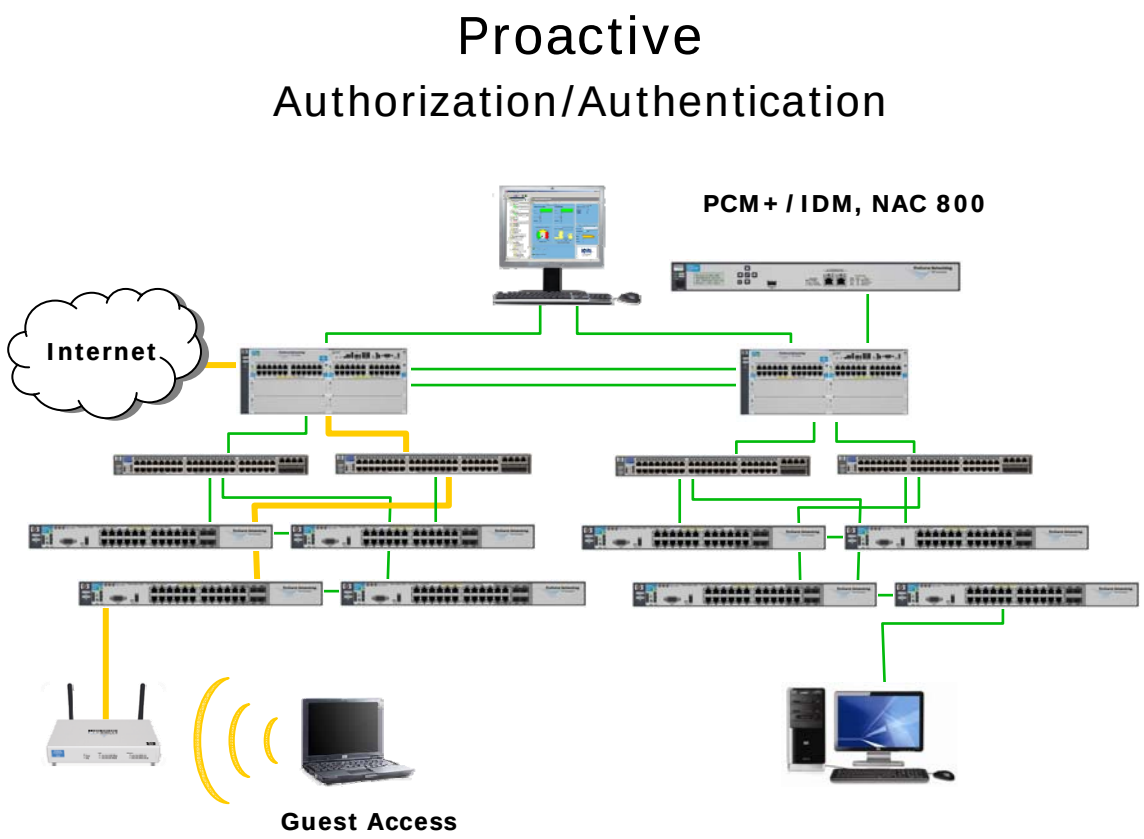


Figure 3: How the "proactive" (access control) aspect of ProActive Defense operates

While the employee and supplier are connected to the network, ProCurve Network Immunity Manager (NIM) monitors their network traffic to ensure both users are complying with network policies.

- For the employee, this means that Internet usage conforms to corporate standards.
- For the supplier, this means ensuring that Web pages on the supplier's network (or other sites that the supplier might visit) do not introduce viruses, Trojans or other malware.

If ProCurve NIM detects a virus or irregular behavior using its built-in Virus Throttle or NBAD technology, it follows preset policies that determine whether to disconnect the user from the network, lower the user's bandwidth, or display a message and wait for the IT administrator to take the necessary action.

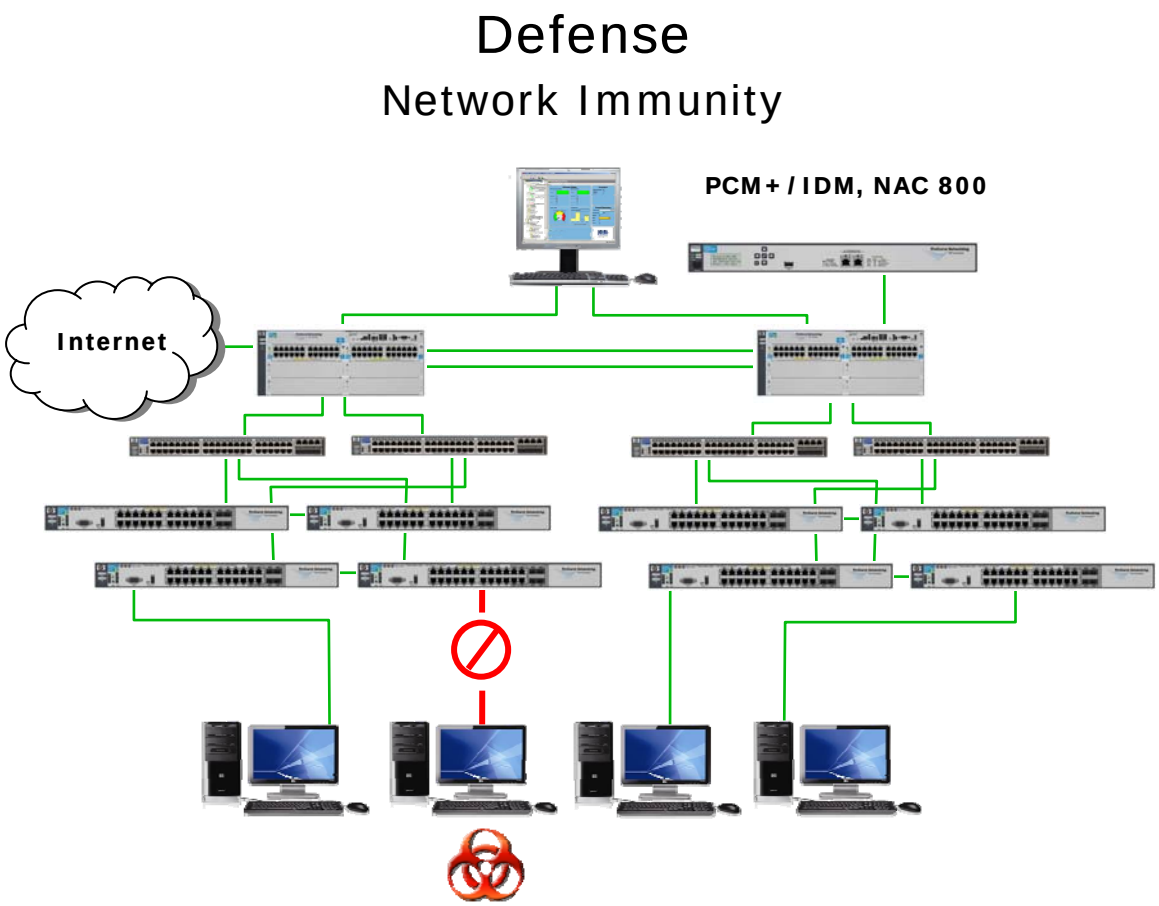


Figure 4: How the “defense” (network immunity) aspect of ProActive Defense operates

Summary

Organizations today rely on their wired and wireless LANs and other networks for the information, processes and resources they need to remain competitive in today’s ever-changing business environment. To protect against the increasing sophistication of network security threats, enterprises must work diligently to adopt a comprehensive security solution.

Securing LANs provides an essential first line of defense against threats. By enabling ProCurve’s ProActive Defense strategy – based on a trusted network infrastructure and encompassing a comprehensive, multi-layered approach that simultaneously combines offensive and defensive security strategies – organizations can protect their networks and optimize networking’s ability to support their business objectives.

With ProCurve ProActive Defense solutions in place, organizations can minimize the risks of downtime and data loss from both internal and external network threats – while taking advantage of the reduced complexity, lower operational costs and increased productivity delivered by the ProCurve Adaptive EDGE Architecture.

To find out more about ProCurve Networking products and solutions, visit our web site at

www.procurve.com

4AA1-8325ENW, 02/2008