

ProCurve Network Immunity Solution

Technical White paper

Introduction	2
Current Security Concerns.....	2
Zero-Day Attacks	2
Rise of Internal Threats.....	3
ProCurve Network Immunity Solution.....	4
What it is.....	4
How it Works.....	5
Threat Detection	5
Threat Mitigation.....	5
ProCurve Network Immunity Manager (NIM)	6
Threat Detection	7
Threat Mitigation.....	7
Security Management	7
ProCurve Switch Security Features.....	8
Virus Throttle	8
sFlow	8
Intelligent Mirroring.....	8
Non-ProCurve Security Devices	9
Summary.....	9

Introduction

Security breaches and regulatory compliance are driving organizations of all sizes to implement strong security measures to protect business-critical data. A single worm or virus can inflict devastating damage to an organization, making it impossible to dismiss the need for a comprehensive security strategy.

Security enforced by corporate firewalls, intrusion prevention systems (IPSs) and virtual private networks (VPNs) has been the first layer of defense against threats. Traditionally these security measures are deployed at the perimeter of an enterprise network to prevent attacks or hackers from the Internet.

Worms such as Blaster, Slammer and CodeRed proved that internal threats pose even greater risk and are more difficult to defend than attacks from external networks or the Internet. With the growing mobile workforce, threats are brought inadvertently into the network by trusted users of the organization (e.g., employees, contractors and business partners) with access to enterprise LAN and WLAN networks.

Today's organizations need a proactive approach to security. The security controls must be built-in to the trusted infrastructure, intelligent to detect known and unknown threats, and able to minimize management overhead to secure complex systems. The ProCurve Network Immunity Solution – part of the overall ProCurve ProActive Defense strategy – fulfills these requirements.

Current Security Concerns

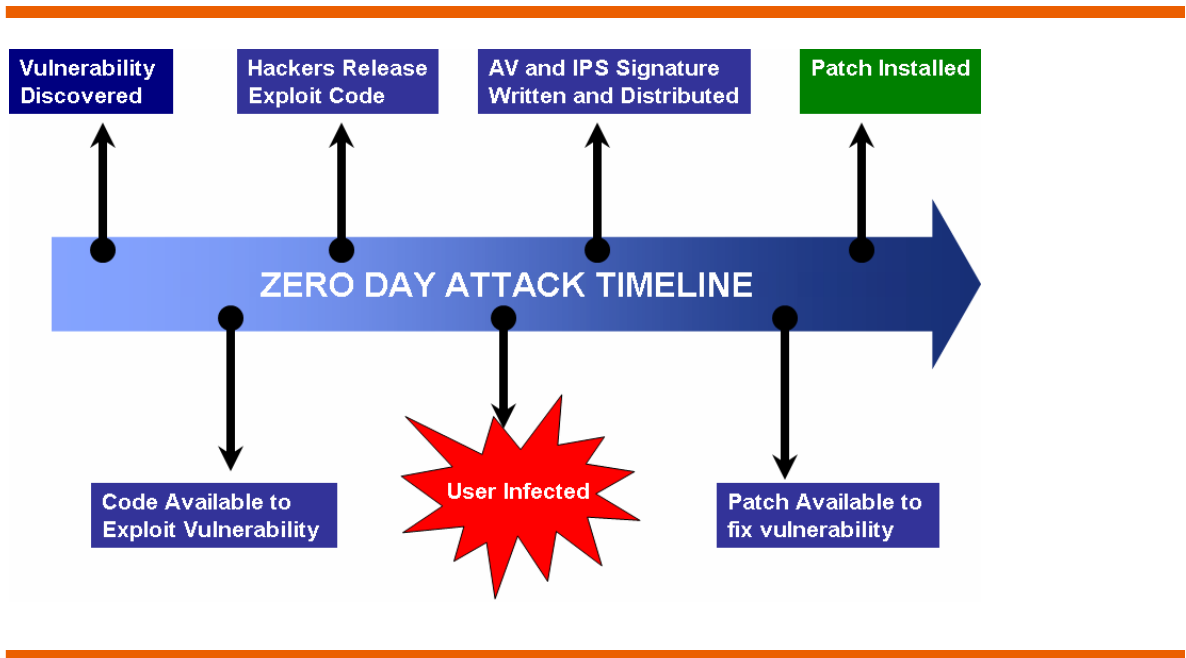
Zero-Day Attacks

Recently there has been a dramatic surge in zero-day attacks¹ on operating systems, Web applications, network devices and client software. Popular tools such as Microsoft Word, Internet Explorer and Microsoft PowerPoint have been the primary targets for such attacks. They are the most commonly used software by employees or contractors of an organization for productivity and messaging purpose.

A zero-day attack is a computer threat that exploits an undisclosed or unknown vulnerability or flaw in the software code before a fix or patch is available.

When a zero day attack is released on the Internet, users of the infected software are exposed to the threat until a software patch or fix is available, or some form of mitigation is taken by the user (e.g., disable vulnerable service). The outbreak of zero-day viruses or worms can span the globe within a day of when the exploit code is released. With increasing hacker sophistication, the time between the discovery of a vulnerability and dissemination of exploit code (virus or worm) is shortening considerably, making it difficult for users to take any sort of mitigation action.

¹ SANS Top 20 Internet Security Attack Targets (2006 Annual Update)



Security products such as anti-virus or intrusion prevention systems that are designed to use virus signature definition cannot detect zero-day attacks, because these attacks involve new or unknown viruses for which a signature or patch has not been written.

To protect against zero-day attacks, security systems must offer network administrators complete network visibility, and they must employ heuristics or network behavior analysis to detect viruses or worms that are new or unknown.

Rise of Internal Threats

Traditionally, organizations relied on the installation of physical security, authentication mechanisms and network security products such as firewalls and intrusion prevention systems to defend against threats. This approach was based on the assumption that hackers or attackers came from an external source such as the Internet or a competitor's network.

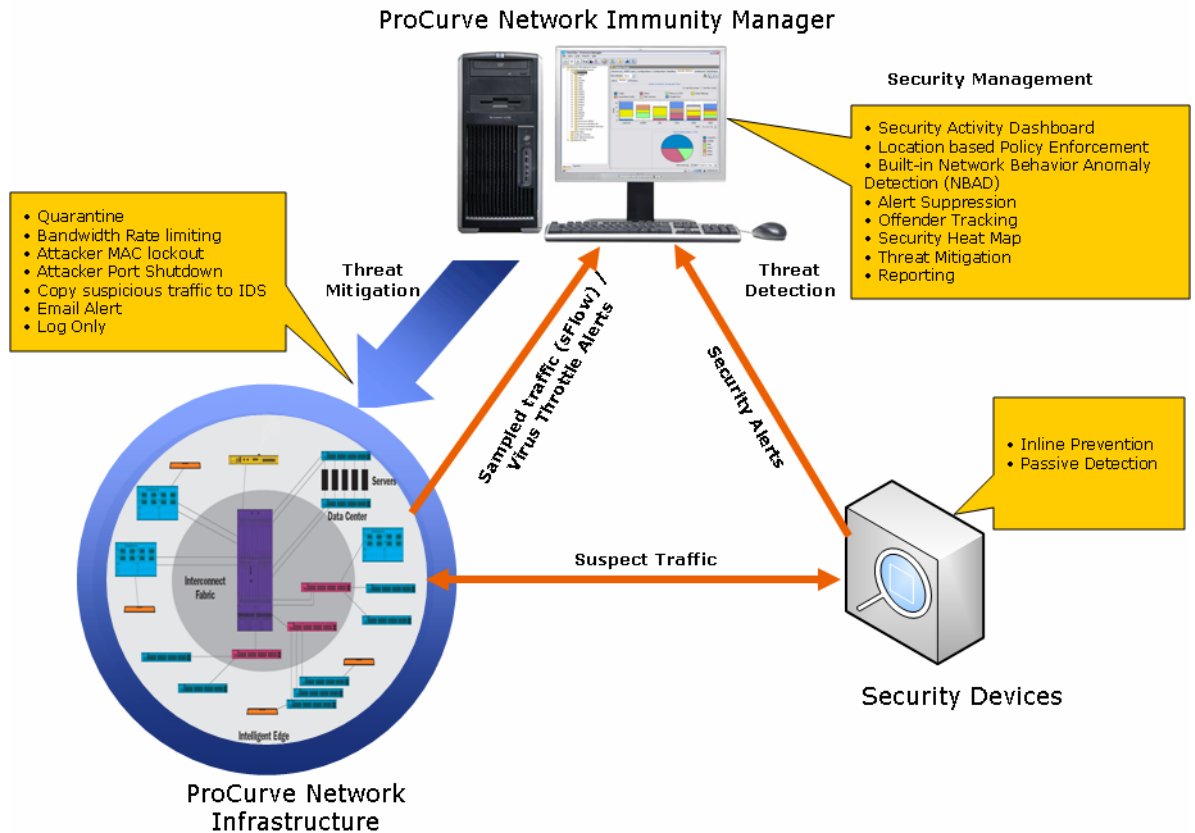
A security breach or virus attacks could also originate from a negligent or malicious employee or contractor, someone with authorized access to the organization's system or familiar with company security policies. Internal threats such as these are as dangerous as attacks from an external source.

Moreover, when a virus-infected employee or contractor system connects to the corporate LAN, the outbreak of the virus is much faster and more difficult to defend because it has already bypassed many of the normal security measures. It could impact every network and sensitive piece of data the employee is authorized to connect to or handle.

Due to growing insider threats, regulatory compliance such as Sarbanes-Oxley (SOX), Basel II, HIPAA and others require organizations to monitor and evaluate internal controls. This compliance ensures that sufficient security measures are in place to protect against internal threats to critical business data.

ProCurve Network Immunity Solution

What it is



ProCurve Network Immunity Solution – which combines the ProCurve Network Immunity Manager (NIM) product, security features built into ProCurve infrastructure devices (switches, routers and wireless access points) and optionally external security devices – provides a comprehensive threat detection and mitigation capabilities across wired and wireless networks.

ProCurve Network Immunity Solution can be seamlessly deployed in an existing ProCurve environment with minimal impact to the live network traffic. Because ProCurve Network Immunity Manager threat mitigation does not require any client agents or software to be installed, the solution is completely transparent to the network’s users.

The location-based policy enforcement capability of ProCurve Network Immunity Solution allows IT administrator to define policies based on the physical location at which the user connects. When an attack is detected, the location of the offender is discovered and the right mitigation actions are enforced based on the policies defined for that location.

The easy-to-use graphical interface walks through various security management processes, such as security policy creation, monitoring events in real time, offender tracking, generating report on security activities and others.

Key benefits of the solution include:

Maximize Network Availability – The ability to detect and automatically respond to virus attacks provides uninterrupted network availability for business users.

Regulatory Compliance Assistance – Various pre-defined reports on security activities and policy controls allow auditors to validate internal controls enforced in an organization.

Integration With Infrastructure – It leverages security features built into ProCurve switches and routers and aggregate alerts from external security devices to detect and mitigate attacks.

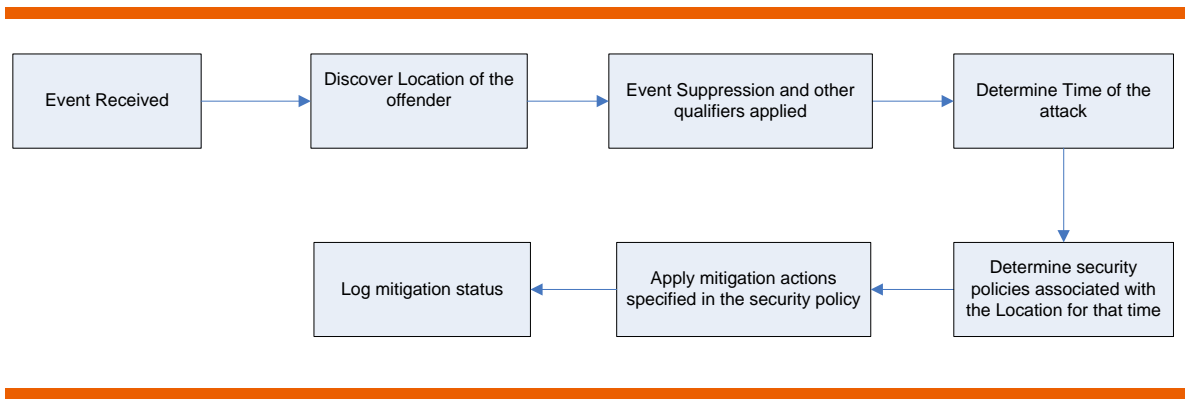
Broad Coverage – Complete network visibility helps detect known and zero-day attacks across wired and wireless environments, simply and requiring few additional components.

How it Works

Threat Detection

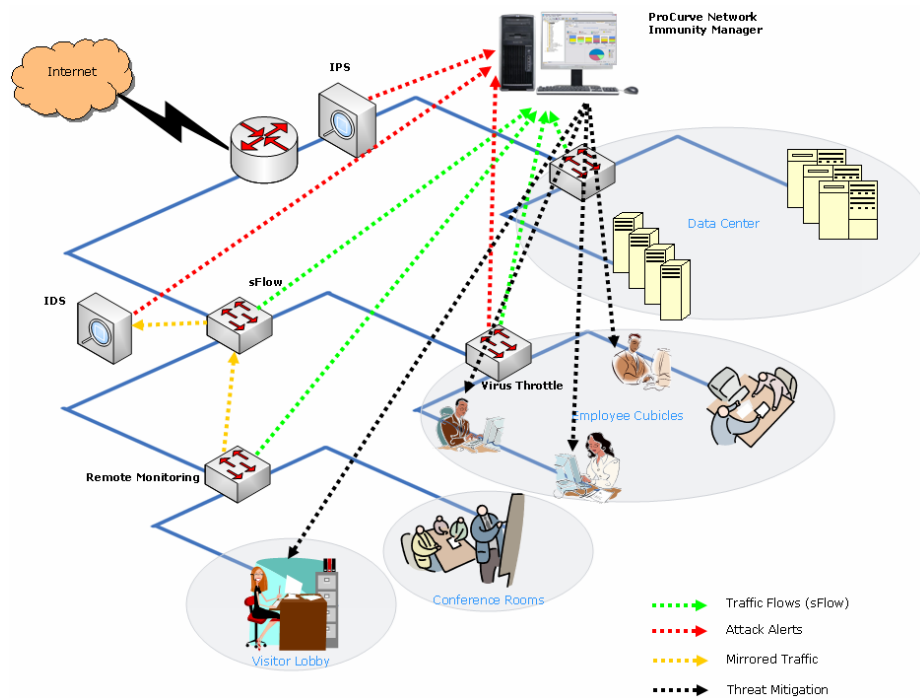
Most ProCurve network infrastructure devices (switches and routers) have sFlow traffic sampling capability built in. ProCurve Network Immunity Manager leverages the sampled traffic flow data to monitor the network, using the network behavior anomaly detection (NBAD) technique to detect suspicious activity. Unlike with anti-virus or most IPS devices, the built-in NBAD engine allows NIM to detect virus attacks without requiring any virus signatures. As a result, ProCurve NIM can detect unknown or zero day attacks for which a signature or patch has not been written.

ProCurve Network Immunity Manger can aggregate alerts from ProCurve intelligent edge switches and external security devices. The aggregated alerts from various security sources are filtered through alert qualifiers defined for that event source to determine if the event is an actionable alert. If it is, ProCurve NIM discovers the location of the offender and time of attack. Based on the security policies defined for that location and time of the attack, the right mitigation actions are enforced and the status is reported.



Threat Mitigation

Once an attack is detected, ProCurve Network Immunity Manager automatically scans the network to discover the port where the attack originated or offender connected. Once the offender location is discovered, actions can be enforced to mitigate the attack.



ProCurve Network Immunity Manager supports a range of actions to mitigate threats when an attack alert is received. Network administrators can choose the action(s) to be taken when the specified alert type(s) identify an offender in the specified location(s) during the specified time frame.

Administrators can provide a prioritized list of possible actions and set up NIM to execute all actions in order, or to stop after the first successful execution. This flexibility is needed because locations may contain a mix of device types; the network administrator could specify an action to be taken that is not possible on all of the devices within the location, so having a list of prioritized actions provides a means to specify preferred actions that are secondary, tertiary and so on for such circumstances.

ProCurve Network Immunity Manager supports the following list of actions:

Quarantine Offender – Add a port to the specified quarantine VLAN.

Offender MAC Lockout – Configure the switch to block the offender MAC address.

Offender Port Shutdown – Shut down the offender port.

Offender Port Rate Limiting – Enable rate limiting at the port.

Offender Port Mirroring – Enable monitoring on the port to mirror traffic to the IDPS system for deeper analysis.

Enable sFlow at the Offender Port - Enable sFlow on the port for deeper analysis.

Email Notification – Send email alerts to the administrator.

Log Only – Log alerts.

ProCurve Network Immunity Manager (NIM)

ProCurve Network Immunity Manager is the main user interface to the ProCurve Network Immunity Solution. It allows network administrators to define policies, collect security events, monitor threats and automate mitigations. ProCurve Network Immunity Manager is an add-on module to ProCurve Manager Plus (PCM+) software; some of the capabilities described in this section utilize or extend PCM functionalities.

Threat detection, threat mitigation and security management are the core functionalities of ProCurve Network Immunity Manager.

Threat Detection

- **Network Visibility** – Monitors traffic across wired and wireless network, using sFlow data from ProCurve infrastructure devices.
- **Multiple Intrusion Detection Methods** – Detects intrusions using virus throttling by ProCurve switches, Network behavior anomaly detection by ProCurve Network Immunity Manager and security alerts from signature-based external security devices.
- **Network Behavior Anomaly Detection** – Detects unknown or zero-day virus attacks by scanning sampled traffic for malicious behavior and protocol anomalies across LAN and WLAN environments.
- **Offender Tracking** – Identifies the offender (username, IP, MAC and DNS name) responsible for the attack, and track user location and network activities. Detailed user session statistics can be obtained if ProCurve Identity Driven Manager (IDM) is installed.
- **Remote Monitoring** – Allows ProCurve switches to mirror suspicious traffic to remote IDS. Monitors traffic across the network using only a few IDS devices.
- **Integration With Non-ProCurve Security Devices** – Aggregates events from non-ProCurve security devices and triggers mitigation actions based on the defined security policy.
- **Security Heat Map** - Provides a real-time view of security activities across the network and pinpoints devices where an attack occurs by visual color coding.

Threat Mitigation

- **Internal Threat Protection** - Discovers the switch port where the internal offender connects and mitigates the attack at the port where the attack originates.
- **Location-Based Policy Enforcement** – Enforces security policies based on the location of the offender and time of attack.
- **Multiple Threat Mitigations** - Mitigates security threats by quarantine VLAN, bandwidth rate limiting, offender MAC lockout, offender port shutdown, email alert or log only.
- **Deeper Analysis** – Reduces false positives by enabling sFlow or mirror traffic to offline IDPS for deeper analysis on alerts that carry a relatively low level of certainty.
- **Chain of Actions** – Prioritizes lists of mitigation actions, so when a response to the attack fails, an alternate response can be triggered.
- **Wireless Support** – Mitigates threats from wireless LANs by blocking the offender MAC address.

Security Management

- **Policy Management** – Creates and manages security policies based on event source, location, time, severity, action and various alert parameters.
- **Security Event Aggregation and Suppression** – Aggregates security events from ProCurve network infrastructure products and non-ProCurve security devices, and suppress duplicate alerts to trigger one action for a flood of alerts.
- **Security Dashboard** – Provides a real-time view of security activities, mitigation actions taken and offender details across the network over various time intervals.
- **Exempt List** – Lists a set of IP address, MAC and DNS names that are exempted from mitigation actions.
- **Configuration Cleanup** – Automatically rolls back response configurations from ProCurve switches and wireless access point after the policy expires.
- **Security Auditing** – Utilizes ProCurve Manager Audit Logging to log any changes to policy configurations and network devices.
- **ProCurve Manager Integration** – Built-in capability manages ProCurve switches, routers and wireless access point configurations and understand network topology.
- **Reports** - Generates network-based, offender-based and alert-based tabular reports with various degree of information granularity.

ProCurve Switch Security Features

Virus Throttle

Virus throttle is based on the detection of anomalous behavior of network traffic that differs from normal activity. Under normal activity, a computer will make fairly few outgoing connections to new computers, but instead is more likely to regularly connect to the same set of computers. This is in contrast to the fundamental behavior of a rapidly spreading worm, which will attempt many outgoing connections to new computers. For example, while computers normally make approximately one connection per second, the SQL Slammer virus tries to infect more than 800 computers per second.

Virus throttle works by intercepting IP-routed connection requests – i.e., connections crossing VLAN boundaries – in which the source subnet and destination subnet are different. The virus throttle tracks the number of recently made connections. If a new, intercepted request is to a destination to which a connection was recently made, the request is processed as normal. If the request is to a destination that has not had a recent connection, the request is processed only if the number of recent connections is below a pre-set threshold. The threshold specifies how many connections are to be allowed over a given amount of time, thereby enforcing a connection rate limit. If the threshold is exceeded, because requests are coming in at an unusually high rate, it is taken as evidence of a virus. This causes the throttle to stop processing requests and, instead, to notify the system administrator or ProCurve Network Immunity Manager.

Virus Throttle is supported on ProCurve Switch 3400, 3500, 5300, 5400 and 6200 Series products.

sFlow

ProCurve switches and wireless edge service modules implement a standards-based sFlow agent (RFC 3176) for enhanced traffic analysis, which provides a network-wide view of traffic patterns that helps predict traffic congestion and allows the network administrator to plan for future upgrades. When used with network management applications such as ProCurve Manager Plus, administrators can monitor overall traffic levels, network segments with the highest traffic or even the top users within a network segment.

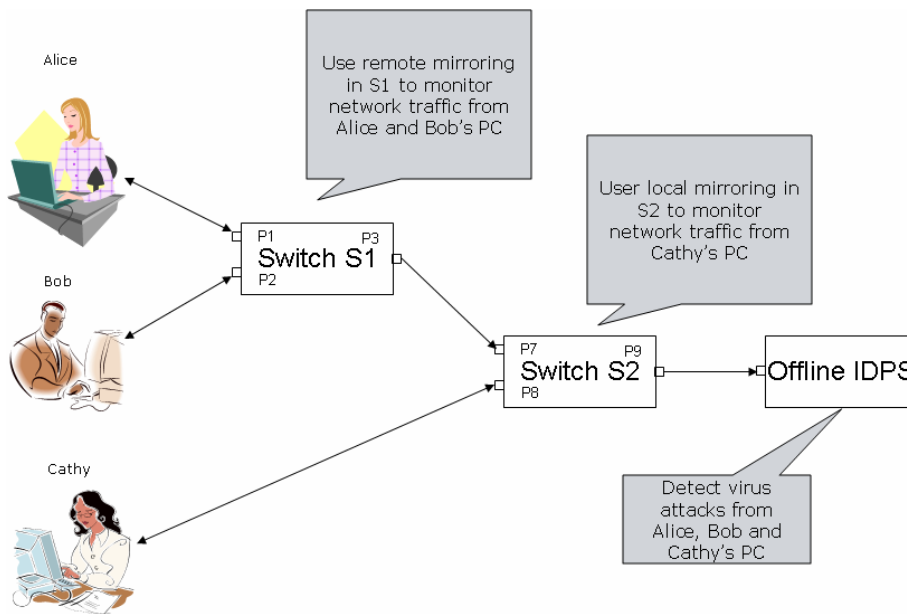
The sFlow data is a key information source for the ProCurve Network Immunity Manager Network Behavior Anomaly Detection (NBAD) engine. ProCurve Network Immunity Manager collects and analyzes sFlow data from various infrastructure devices such as switches, routers or wireless access points to detect malicious activities or zero-day attack behaviors.

sFlow supports ProCurve 1600, 2400, 2524, 2800, 2810, 2900, 3400, 3500, 4200, 5300, 6200, 8000, 9300, 9400 products, as well as the Wireless Edge Service Module.

Remote Mirroring

The network activity on a switch can be monitored using local and remote mirroring functionality. As the names imply, local mirroring allows a network analyzer to monitor local switch traffic, whereas remote mirroring allows monitoring of remote switch traffic. The table below lists the differences between local mirroring and remote mirroring:

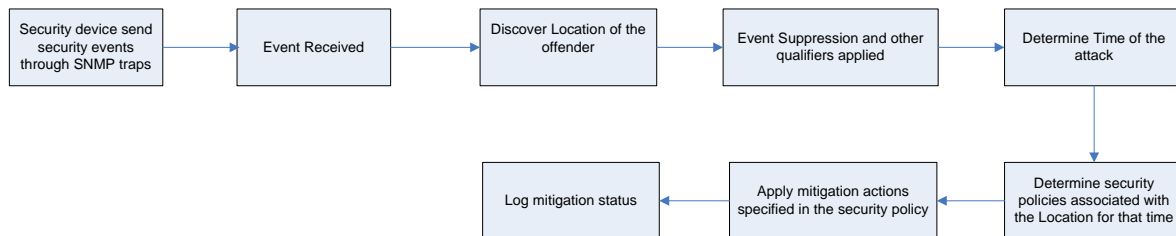
Local Mirroring	Remote Mirroring
Used when an IDPS (Intrusion Detection and Prevention System) that monitors traffic for intrusions is connected to the local switch port.	Used when an IDPS that monitors traffic for intrusions is connected to a remote switch.
Mirrors traffic directly to IDPS.	Mirrors traffic to a remote switch where IDPS is connected.
Supported in switches with Basic Mirroring and Intelligent mirroring functionality.	Supported only in switches with Intelligent mirroring.
Supported in most ProCurve products.	Supported in ProCurve 3500, 5400 and 6200 products. Requires remote mirroring source and destination switch to be a ProCurve 3500, 5400 or 6200 product.
Tunneling not required.	Requires an IPv4 tunnel that encapsulates packets from a source switch (monitor traffic) to a destination switch (with IDPS).



Local and Remote mirroring usage

Non-ProCurve Security Devices

ProCurve Network Immunity Manager can consume and aggregate events from non-ProCurve security devices through SNMP traps (v1/v2/v3). The security events are filtered through various alert qualifiers defined for that event source to determine if the event is indeed an intrusion alert. If so, Network Immunity Manager discovers the location of the offender and the time of attack. Based on the security policies defined for that location and time of attack, the right mitigation actions are enforced and the status is reported.



Summary

Growing mobile workforces and increasing numbers of wireless users not only make security much more complex, but they also make security even more critical. Computers and networks have become integral to business operations, and having a network disruption for a single day could bring huge loss in money and reputation.

In response to recent years' corporate scandals, regulatory compliance such as SOX, HIPAA, GLBA, FISMA and PCI require businesses to comply with internal control requirements. Companies are forced to demonstrate compliance with security requirements, from both regulatory bodies and internal mandates. For many organizations, compliance has become a top security concern.

To meet current security concerns, organizations need a comprehensive security strategy that integrates with their existing infrastructure, enforces internal controls and reports security activities for auditing and forensics purpose.

ProCurve Network Immunity Solution, a key aspect of ProCurve ProActive Defense, is an approach that delivers an integrated wired and wireless security solution that includes threat detection, threat mitigation and security management capabilities. It 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.

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

www.procurve.com



© 2007 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.

4AA1-0788ENW, 02/2007