



hp procure  
networking  
business

january 2003



business  
white paper

## hp procure enterprise network security readiness protecting investments with the hp procure adaptive EDGE architecture

### table of contents

introduction	2
what network security means today	3
forces in the network security landscape	3
mobility	4
convergence	5
protecting the network	5
control to the edge is a key factor	6
HP ProCurve's security solutions	6
value proposition	10
summary	10
for more information	11

## introduction

Network security has never been more important to enterprise companies. The Computer Security Institute's (CSI) and FBI's 2002 annual Computer Crime and Security Survey reported that 90 percent of major corporations and government agencies detected computer security breaches in the previous 12 months. Survey respondents' average loss was \$6.6 million. "Post-9/11, there seems to be a greater appreciation for how much information security means not only to each individual enterprise but also to the economy itself and to society as a whole," remarked Patrice Rapalus, CSI Director, in a recent media announcement.<sup>1</sup>

As security has risen in awareness, so too have the matters that complicate it. No longer simply a 'check box' item, network security has become a top priority for enterprises and the focus has expanded from just the Internet connection to the enterprise LAN as a whole. Many key technology trends are increasing the intricacies of network vulnerabilities and security enforcement, including:

- the numerous ways to access enterprise network applications and resources;
- a variety of user types with access;
- an increasingly mobile work force with a vast number of wired and wireless devices;
- internal and external security threats both accidental and intentional;
- a move toward multi-service networks using next-generation communication applications
- hacker tools and debilitating computer viruses that are readily available and sometimes unintentionally disseminated.

All of these factors significantly impact an enterprise's network security and information asset protection.

It is no longer adequate to have exclusively centralized host-based security with Internet firewalls and intrusion detection. In today's unpredictable business climate, enterprises must have a security strategy that includes detection and enforcement at every point of network access, for all user types. This means providing intelligent access services at the edge of the network, where users connect — whether it is via a switch in a wiring closet or a wireless access point. Network and policy management, however, remains centrally managed for crucial control. Not only does network-based access ensure secure, quick, and appropriate access for authorized users to only the services they need, but it also stops unauthorized users from connecting to the network. If a malicious user can infiltrate the network and gain intelligence regarding private resources, it's possible to launch attacks on information assets, users and even the network itself.

HP ProCurve networking solutions have several layers of built-in security. The company has heavily invested in ensuring that HP products comply with the newest and most stringent standards to protect data; in fact, HP leads the establishment of many of these standards.

This paper provides an overview of the network security issues executives and IT managers face as enterprise networks become more public, more converged and more mobile. It will illustrate the strong need to support new security methods and the advantages of providing security access control at the network edge.

---

<sup>1</sup> CSI. "Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row." April 7, 2002. Press release.

## what network security means today

Security used to mean setting up a firewall as a perimeter line of defense to keep trusted users on the inside and untrusted users on the outside. But in today's world of remote workers, wireless users, trading partners, customers and hackers, that perimeter line has been blurred beyond recognition. The perimeter or point of contact with the Internet is still important but it is not sufficient in providing end-to-end network security. An effective security strategy needs to be far more flexible and sophisticated than just posting a guard at the gate to your network. The new model for network security calls for protecting data wherever it is and trusting no one completely wherever they are.<sup>2</sup>

In terms of dollars, a network security breach can mean billions of real and future revenues lost. The price paid often includes both direct and indirect costs and is measured by damaged sales, consumed IT staff resources, lower user productivity levels, lost intellectual property if trade secrets are stolen, decreases in public confidence and lost business opportunities and revenue.

In terms of wired and wireless networks, access control is a significant issue as it is common to have pervasive, live ports nearly everywhere within an enterprise campus. Where enterprises once had a one-to-one correspondence between an access port, a PC and a user, today's LANs extend beyond the controlled office environment. The emergence of numerous mobile network access devices, next-generation convergence solutions and inexpensive wireless access points, combined with open ports existing in many campus public areas, provides endless connectivity opportunities. It is critical that enterprises understand that wireless security solutions will not be entirely effective if the enterprise wired LAN security is not airtight. If the wired network is not secure, it is simple to plug-in a wireless access point that can go undetected and provide endless access to multiple users.

In terms of network strategies, creating security solutions that bring peace of mind means having an adaptive network model that controls which users perform which tasks based on the needs of their job. Enterprises should consider their network security like airports. People come and go at all hours, some areas are more secure than others, and as people pass from one area to another they have to present their credentials: tickets, boarding passes or passports. Apply this approach to computer security, and instead of an "exclusive" model in which organizations try to prevent people from doing things they shouldn't, they have an "inclusive" model that seeks to provide appropriate access.<sup>3</sup>

With HP ProCurve networking solutions based on the HP ProCurve Adaptive EDGE Architecture, security means creating intelligence throughout the enterprise network to the edge where the user connects. This approach enables enterprises to mitigate risks more effectively as they protect their digital assets. Furthermore, it allows cost effective partitioning of the network to create zones of similar users with similar access needs.

## forces in the network security landscape

As businesses increasingly rely on the Internet and networks, enterprise networks are figuratively, and in some cases literally, becoming one public network. This shift makes enterprise data and communication systems even more vulnerable to security threats. The global economy and the technology trends shaping it have changed the networking landscape forever.

In the earliest days, security was simply a matter of locking the door to the server room. Today "locked doors" can be opened with readily available hacking tools and malicious

---

<sup>2</sup> Gaspar, Suzanne. "The New Security Battle Plan." *Network World*. September 30, 2002. Article.

<sup>3</sup> "Securing the Cloud." *The Economist*. October 26, 2002. Article.

viruses. As a result, network managers are continually working to increase not only what needs to be secured, but also how it is secured, who will have what level of access and how users will gain access. Enterprises are learning that providing connectivity and gaining access to network resources are two entirely separate notions, and authorized access is only the tip of the iceberg to the challenge of network security. Without the proper safeguards in place, gaining access to enterprise network applications and resources can be easy for unauthorized users.

Advances in work force mobility and multi-service networks, along with the proliferation of the Internet, are complicating enterprise network security. The interdependencies of these forces create efficiencies for businesses but also make networks more vulnerable. Further aggravating the problem is that network security is a continuous process and investments are made across large, often geographically dispersed, environments. Enterprise network architectures must be multi-dimensional and flexible enough for an enterprise network to support new security methods, new applications and new connection management solutions for the increasingly mobile workforce. They are among several industry trends posing increased complexity for enterprises and their networks.

- **A myriad of ways to access corporate resources:**

Today there are innumerable methods to access enterprise network applications and resources, including wired clients that access the network via switches and routers; wireless clients that connect to 802.11 access points; dial-up clients using the Internet and virtual private network (VPN) software or via remote access services (RAS).

Security applications that control ports and portals may become ineffective as mobility is brought into the network mix. As far as network security is concerned, "Who are you and where did you come from?" has taken the place of "How did you get in here?"

Connection management, along with security is necessary to provide users with location independent services and communication. Supporting secure *mobility* across a range of transports both wired and wireless, inside and out of the office is becoming a key element of a secure network.

- **A variety of user types:**

The management of user types becomes increasingly more complex as the enterprise network environment expands and changes to include full, part-time and temporary employees, contract workers, remote workers, partners, resellers, and customers. Each user type requires different access abilities and network resources.

- **An increasingly mobile work force:**

Wireless networks and devices make the security challenge obvious. A survey by Computerworld found that 30% of American companies had identified rogue access-points on their networks. If these are left open, they provide a back door past the firewall into the company's network.<sup>4</sup> The range of potentially mobile and always mobile digital appliances continues to diversify and proliferate. The network is extending its reach to provide mobile connectivity with local wireless technology, public high-bandwidth wireless hotspots and digital cellular to address

## mobility

---

<sup>4</sup> "When the door is always open." *The Economist*. October 26, 2002. Article.

the needs of anytime, anywhere communications.

## convergence

- **The move toward convergence readiness:**  
As voice, video and data convergence is introduced to the network, new policies and procedures must be put in place. Core network security applications that performed well scanning and policing data transactions may now cause problems for voice and video applications sensitive to latency and jitter. This raises a whole new set of security issues in conjunction with providing quality-of-service (QoS) for a whole new set of applications.
- **Network security is much more than implementing security products:**  
Enterprise LANs are the lifeblood of most businesses today. Thinking must shift from resource and application safeguards to a multi-layer approach for complete network protection. This is a shift in the way enterprises view network security.
- **Network security can be expensive and does not produce revenue**  
Even though security is top-of-mind for many IT executives and staff, it is still perceived by some as a necessary evil and a resource drain. Price is a major concern as an ongoing security strategy can be expensive and does not produce revenue. However, much like insurance, network security is necessary and network managers are not hesitating to increase spending to bolster their defenses.

## protecting the network

Where a network manager used to be concerned only with external threats, today's network manager must also be concerned with internal problems, both real and potential. Unfortunately, it's no longer a given that anyone with authorized network access is completely trustworthy. Companies must implement network-based security with zones for different users combined with the conventional host-based security and Internet firewalls.

As Ethernet extends into the far reaches of every campus corner, wired active ports are nearly everywhere. Controlling access to valuable information is a key requirement and a challenge to provide authenticated roaming across wireless LAN subnets. With standards like 802.1X port based access control – established with HP ProCurve leadership – security begins when a user plugs in a cable. In addition, with 802.1X, access will only be granted if the user is authenticated against a secure database.

Furthermore, the network can control which virtual local access network (VLAN) the user should be placed on to restrict access to certain systems and services based on the user's profile. VLAN's can be used to divide the enterprise LAN in multiple sub-networks that are isolated from each other. Users on one VLAN cannot access resources on other VLANs without authorization and appropriate control of the network itself.

As enterprises depend more and more on Ethernet LANs for all kinds of communication, they need to protect the network itself from attack. Certainly, physical security of wiring closets and equipment rooms is necessary, but enterprises must also secure management access to the infrastructure. It is vital to implement an enterprise LAN with switches that offer the latest in management security.

**control to the edge is  
a key factor**

Closely examining the issues associated with QoS in a secure mobile environment suggests that the best method for securing control and functionality is to implement it at the edge of the network. Security must be enforced when the user connects at the edge of the network via a wired office connection, a wireless LAN connection or from a remote location via an ISP.

New applications will require QoS, traffic conditioning and rate limiting to allow them to all coexist on one network. Such control must be established at the edge and maintained across the network. For example, as a user moves from one location to another, the edge must preserve the connection as appropriate from wired to wireless, in the office to out of the office and back again, all while continuously enforcing security. *Control to the edge* via HP ProCurve's Adaptive EDGE Architecture is the only way to offer full support for today and tomorrow's new applications, while also ensuring secure, quick and appropriate access and mobile connectivity to services and information.

In addition to providing control to the edge, defining who gains access to which applications, services, and information is a policy decision driven by an organization, its mission, job descriptions, customer profiles and more. *Control to the edge* must be paired with *command from the center* driven by business needs and priorities.

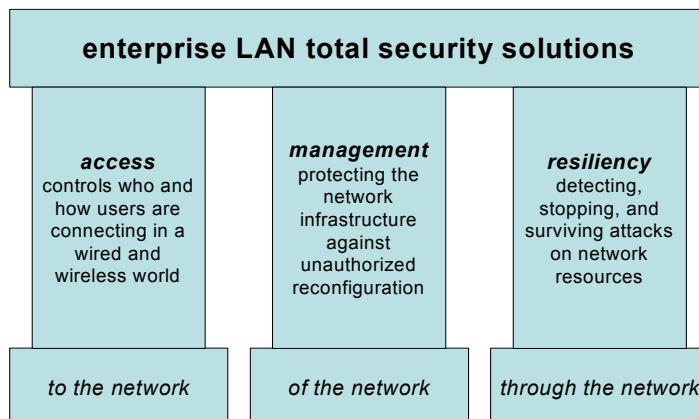
**HP ProCurve's  
security  
solutions**

For nearly 20 years, HP ProCurve has been building enterprise LAN products that help customers run their business more effectively. The company has a complete and affordable portfolio of security solutions and services for its customers. HP ProCurve security solutions allow important network access decisions to move to the edge of the network where users and applications connect.

As mentioned, security enforced at a central point gives malicious traffic an opportunity to infiltrate the network from the edge to the core. Stopping any unauthorized or suspicious activity at the edge or access point immediately isolates the problem and therefore reduces the chance that the network as a whole will be impacted. This approach prevents users from gaining unauthorized network knowledge or performing electronic snooping to uncover passwords or other critical information that might assist in a network attack. HP ProCurve's Unified Edge Access secures all end-user access methods to the enterprise LAN (figure 1). If a security breach cannot infiltrate the host because network intelligence locks out the potential attacker, enterprise network security improves dramatically.

HP ProCurve's security to the edge solutions includes a framework of access security, management security and attack resiliency (figure 1).

# HP ProCurve framework



**Access security** controls who and how users are connecting in a wired and wireless world.

- Standard 802.1X port based access control is available on all HP ProCurve enterprise class managed switches. These state-of-the-art access control mechanisms are enhanced by additional capabilities found in ProCurve switches such as MAC lockdown and source port filtering to only provide access to appropriate users and protect open ports from inappropriate use.
- Combining 802.1X with 802.1Q standards provides two levels of security. When a user authenticates via 802.1X, ProCurve switches can easily place the user on the appropriate VLAN based on information contained in the RADIUS server. Authorized users can be limited in exactly which network resources they are allowed to access. If the authentication fails the switch can be configured to put the user on a guest VLAN.
- 802.1X is also used with 802.11 wireless networks to insure only authorized users are granted access to the enterprise network. Additionally, 802.1X enables a mechanism of dynamically distributing per-user encryption keys for use with the latest native 802.11-encryption schemes ensuring that traffic cannot be monitored or listened to by attackers.

ProCurve access control switch features at-a-glance
<ul style="list-style-type: none"> <li>• 802.1x port based access control using RADIUS server for authentication</li> <li>• MAC lockdown</li> <li>• source port filtering</li> <li>• 802.1Q VLANs with per-user port VLAN assignment</li> <li>• access control lists</li> </ul>

**Management Security** includes the protection of the network infrastructure itself and prevents unauthorized users from overriding other security provisions. This means that only the network managers responsible for administering the network can make changes to the

network configuration.

- Securing *controlled* access to the configuration and management to the network infrastructure is critical. This is why HP ProCurve switches support the latest in management access security.
- ProCurve switches can authenticate network managers in a number of ways. An encrypted database embedded in the switch flash file-based system stores usernames and passwords for both manager-level and operator-level users. These same users can be authenticated against an external database for a second confirmation of the user's authenticity.
- Remote management access to the console prompt is protected using the secured shell protocol (SSH). Additionally, access to the Web user interface is secured using the secured sockets layer (SSL). The benefit is that the traffic between the management console and the switch cannot be listened to enabling anyone to get information about the network or impersonate a network manager.
- To control how and where remote management occurs, ProCurve switches support standards and protocols from a control list of authorized IP addresses or subnets. A dedicated management VLAN can be configured to restrict access to management functions from other VLANs configured within the device. This creates a secure management domain that further ensures that only authorized network managers can configure the network.

**ProCurve management security switch features at-a-glance**

- a local username/password encrypted database for manager and operator level users
- TACACS+ (like the RADIUS protocol but Cisco proprietary)
- secure socket layer (SSL) (encrypts management traffic over the wire for the web agent)
- secure shell (for encrypted telnet connections)
- authorized managers list (limits the management stations that can communicate with the switch using an IP address and net mask)
- a dedicated management VLAN
- SNMPv3 (adds encrypted passwords and management authentication, scheduled for release Jan 1)
- HP TopTools provides levels of management access user access levels
  - default user (view but not change)
  - operator (some change control but can't change passwords)
  - administrator (full control including passwords)

**Attack Resiliency** is about creating a more reliable and available network infrastructure designed to survive a network attack without interrupting service or going down.

- While securing the perimeter of the network with access control techniques and securing network devices with management access techniques goes a long way to securing a network, both intentional and unintentional network attacks may still occur. Network-based viruses can infect authenticated laptops and PCs when connected to the Internet outside of the office. These viruses, in addition to attacking network components, can compromise the network from

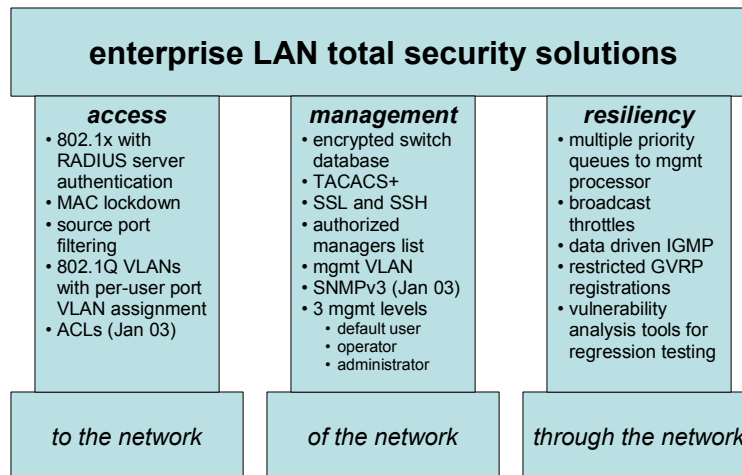
within. ProCurve switches come with a number of built-in features that improve the resiliency of the network in the face of such virus outbreaks.

- The management functions of ProCurve switches are protected from broadcast storms, flooded traffic, network loops and overloaded links by an advanced packet classifier that directs traffic to one of many paths to the CPU. This resilient traffic classifier enables access to switch management in the presence of these network anomalies.
- Broadcast traffic impacts every station on the network, and excessive broadcast traffic is typically an erroneous situation. ProCurve switches can reduce broadcast traffic using a per-port ASIC-based broadcast throttling mechanism.
- High-bandwidth multimedia streams using IP-Multicast can flood a network if left uncontrolled. ProCurve switches automatically create and enable IP-Multicast traffic filters based upon intelligent listening of IP-Multicast data as well as participating in the IGMP protocol.
- VLANs are used in most networks to create isolated and controlled network segments. The GVRP protocol enables the dynamic registration and creation of VLANs. The default behavior of this standard is to allow anyone to register and create a VLAN within the network. In many environments, this is not desirable behavior. Network administrators prefer to define and control the creation and propagation of the VLAN topology. ProCurve switches have the ability to restrict VLAN registrations to a set of VLANs defined by the network administrator. This prevents inappropriate or accidental creation of VLANs by unauthorized users.
- ProCurve firmware releases run through extensive testing before being distributed. One of the many standard regression test suites includes the CERT vulnerability test suite. This suite bombards the switch with a number of well known network attacks. Firmware releases are not shipped unless tests are passed.
- Routing protocols control the topology of the network, and unauthorized routing updates could bring a network down. ProCurve routing switches support authenticated routing updates from authenticated routers.
- The 802.1Q standard allows overlapping VLANs in some configurations. Such configurations can be considered a security breach for networks that use VLANs to isolate traffic. ProCurve switches prevent such configurations by automatically configuring VLAN ingress filters.

**ProCurve Network attack resiliency switch features at-a-glance**

- multiple priority queues to the management CPU
- broadcast throttles
- data driven IGMP
- restricted GVRP registrations
- vulnerability analysis tools (e.g. attacker tools) used in regression testing

# hp procurve security today



## value proposition

HP ProCurve Networking solutions meet customer needs by consistently delivering on the value propositions of high availability, affordability, security, ease-of-use and interoperability. The company has a proven track record of invention and experience that allows it to deliver an adaptive and affordable infrastructure for today's and tomorrow's enterprise networks.

HP ProCurve security solutions move important access decisions to the edge of the network where users and applications connect. Core resources are freed to provide the high bandwidth interconnect functions they are meant for, which means enterprise networks are optimized to perform better. What is more, effective control to the edge helps enable the support necessary for network convergence and a mobile workforce.

## summary

It's inevitable. Security will remain a vital component for the viability of network and information systems. Information security is and will continue to be absolutely critical as real-time communication needs increase, the workforce becomes more mobile and enterprises prepare and implement multi-service networks.

Establishing effective network security requires solutions that adapt to new and existing vulnerabilities, minimize risks, and protect information assets at any cost. The HP ProCurve networking business is the leader in providing cost-effective, secure solutions that are easy-to-manage and do not compromise network functionality. What is more, HP ProCurve security solutions move important access control to the edge of the network where users and applications connect. The business benefits of this approach include:

- increased user productivity with quick and appropriate access for authorized users to only the services they need
- more control over who and how users are connecting in a wired and wireless world
- prevention of future attacks and minimized risks as intelligent access services stops unauthorized users from accessing the network.

HP ProCurve Networking products have several layers of built-in security and take advantage of the latest standards-based security features to protect data. HP's diverse array of security products and services bring trust, reliability and flexibility to enterprise networking.

**for more  
information**

More information about HP ProCurve Adaptive EDGE Architecture is available at <http://www.hp.com/rnd/architecture>.

More information about HP ProCurve networking solutions and products is available at <http://www.hp.com/go/hpProCurve>.

HP is a leading global provider of products, technologies, solutions and services to consumers and businesses. The company's offerings span IT infrastructure, personal computing and access devices, global services and imaging and printing. HP completed its merger transaction involving Compaq Computer Corp. on May 3, 2002. More information about HP is available at <http://www.hp.com>.