



# *the* SENTINEL

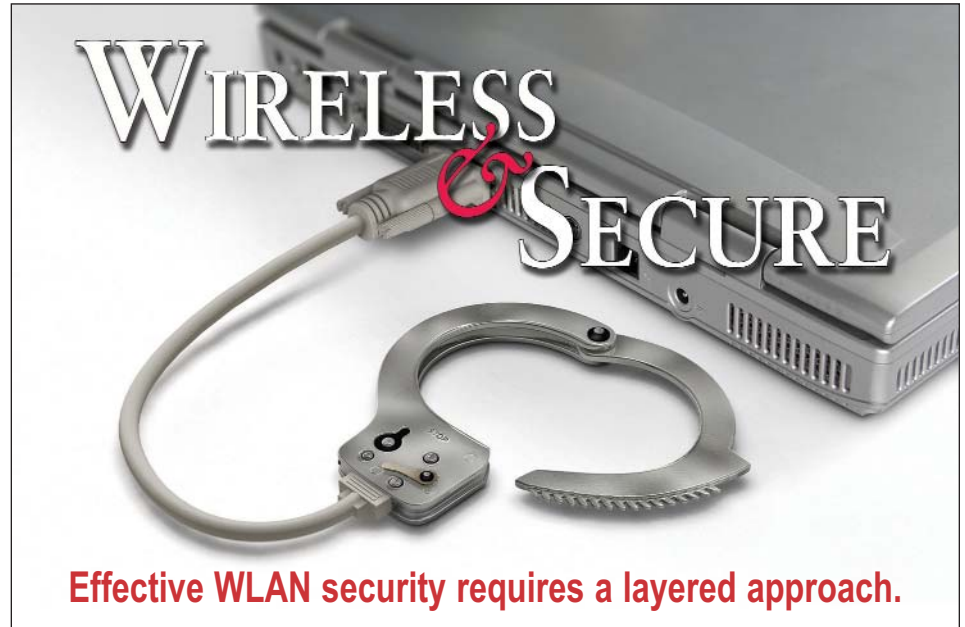
POWERFUL NETWORK DESIGN, SECURITY AND ACCESS CONTROL SOLUTIONS

**T**here's no question that wireless LANs (WLANs) offer compelling benefits in terms of mobility and productivity. Unfortunately, concerns about WLAN security often create a major stumbling block that prevents organizations from fully reaping the rewards of wireless.

The good news is that it's possible to balance mobility with robust infrastructure security. While some organizations have chosen to focus on the risks associated with WLANs — to the point of banning the technology — many others have successfully deployed wireless networks that are as secure as the wired infrastructure.

The key, according to the experts at Classic Networking, is to take a layered approach to WLAN security by identifying and protecting against wireless-specific vulnerabilities. All too often, organizations focus on one area of WLAN weakness — such as inadequate encryption — while failing to see the big picture.

“Effective WLAN security depends upon a comprehensive framework covering all aspects of the wireless infrastructure, from the radio frequency layer all



the way to the application layer,” said Jeffrey Reed, President, Classic Networking. “Organizations must put tools in place that check for rogue devices entering the airspace, attacks on wireless links, and unauthorized users attempting to access the network.”

This requires a mix of security solutions based upon industry standards along with continuous real-time monitoring and policy enforcement. According to

Reed, HP ProCurve wireless products effectively address WLAN vulnerabilities while reducing the cost and complexity associated with wireless networks.

## Know Your WLAN

The lure of wireless combined with the ease with which it can be deployed represents one of the biggest threats to WLAN security. For a small investment, an end-user can introduce a consumer-grade wireless access point into the network, exposing the entire infrastructure to easy attack. Wireless-equipped laptops can pose an even greater threat if not properly secured.

The first step in securing the WLAN is to find rogue access points and either eliminate them or ensure that they meet security standards. Many network administrators will use a handheld “sniffer” and walk through the WLAN coverage area

CommunicationWorks

PRSR1 STD  
U.S. POSTAGE  
PAID  
Tulsa, OK  
Permit No. 2146

*continued on page 2*

## Wireless and Secure

continued from p. 1 ...

looking for wireless data transmissions. However, experts say this is one of the least effective ways of eliminating rogue equipment — new rogue access points can be added after the scan.

“ProCurve Mobility Manager, a plug-in module for ProCurve Manager Plus, provides a rich toolset to manage a ProCurve WLAN environment — including rogue device detection and alerts, wireless client association and health visibility, and template-driven device group configuration and management,” Reed said. “All of the ProCurve Mobility Manager capabilities are seamlessly integrated into a single management console to offer unified management of wired and wireless network resources.”

The next step is to ensure that the WLAN is protected against attack. Reed recommends that organizations install WLAN-specific intrusion detection systems (IDSs) to keep hackers from accessing the wired network via the WLAN. WLAN IDSs continuously monitor 802.11 protocols for security policy violations, known attack signatures and statistical anomalies. They are able to detect and thwart man-in-the-middle attacks, MAC spoofing and unusual activity.

Security software should be installed on all wireless-equipped devices to alert the network administrator of any vulnerabilities. Only enterprise-class access points with robust security should be used, and they should be configured to limit which stations can connect to them.

### What's Your Policy?

It's critical that organizations develop — and enforce — a WLAN security policy that defines access rights and prohibits users from circumventing these measures. However, because most WLANs are designed with end-user mobility and productivity in mind, the challenge for IT staff is to develop security options that support end-user requirements.

“A WLAN security policy must be flexible in terms of the technologies it can support. WLANs enable access by laptops, PDAs, smart phones and more, each with different features, capabilities and security requirements. This diverse set of clients cannot be secured with a ‘one size fits all’ policy,” said Reed.

For example, ProCurve Identity Driven Manager (IDM) policy management tool provides network administrators with the ability to centrally define and apply policy-based network access rights that allow the network to automatically adapt to the needs of users and devices as they connect, thereby enforcing network security while providing appropriate access to network users and devices.

WLAN security policies must also integrate with the organization's wired network security scheme to ensure seamless protection across the organization. While WLANs present unique security challenges, it still boils down to controlling who has access to specific information. Understanding WLAN-specific vulnerabilities and deploying a suite of tools to minimize them enables organizations to enjoy the mobility and productivity benefits of WLANs without putting business-critical applications at risk.



## Network Worries?

Let us put your mind at ease  
with a full network assessment.

As organizations, network configurations, applications and the outside world change regularly, the risks within a network change. Our goal is to present your team with a clear view of the risks associated with operating the network in its current state. Optional components of a network vulnerability assessment include:

- ◆ External Network Assessment
- ◆ Internal Network Assessment
- ◆ Physical Security
- ◆ Aggressive Anti-Virus Scanning
- ◆ Monthly and Quarterly Health Check
- ◆ Wireless Discovery
- ◆ IDS Sampling

Our network vulnerability assessments free up your staff to concentrate on their primary business activities, verifies your existing security policies, and guards against human error in software and hardware configurations. Contact us today to learn more!



(877) CNI-9250  
[www.classicnetworking.com](http://www.classicnetworking.com)

# INTRUDER ALERT

Intrusion prevention systems help thwart network attacks.

Medieval security might seem primitive by today's standards, but it was quite effective in its day. Castles were surrounded by a high wall and moat (dragon optional), and a sentry was posted at the gate to demand the identity of a visitor before lowering the drawbridge. This protected the castle from attack while permitting the comings and goings needed for the day-to-day operation of a kingdom.

Modern-day network firewalls have supplanted the castle wall and moat, and do a pretty good job of keeping out most of the traffic that may pose a threat to the organization. However, most firewall policies specifically allow any network traffic — SMTP, HTTP, FTP, etc. — the organization needs to do business.

Some organizations do post a sentry, known as an intrusion detection system (IDS). However, this sentry isn't able to operate the drawbridge. An IDS is a passive system that sits outside the data path looking for possible attacks within the traffic allowed through the firewall.

Intrusion prevention systems (IPSs), in contrast, sit inline to effectively monitor and block malicious traffic. While IDSs spot incoming attacks and notify administrators, IPSs go a step further by

stopping attacks before they make their way into the network. Because IPSs operate within the data path, they can actively drop packets when malicious activity is identified.

"Ongoing problems with viruses, worms and hacker attacks point to the limited value of IDSs," said Jeffrey Reed, President, Classic Networking. "While it is important to know when an attack is in progress, such notification is not sufficient protection against rapidly spreading attacks. Organizations need inline IPS technology that can both notify of attacks and thwart a potential security breach before it can adversely impact a business."

## Halt! Who Goes There?

When one thinks of an intrusion, one generally thinks of unauthorized network or application access with the intent to steal or destroy valuable information. However, unauthorized access isn't the only intrusion blocked by an IPS.

IPSs use a wide range of techniques — including signature matching and protocol and traffic anomaly detection — to protect against malicious content such as viruses and spyware. IPSs provide real-time protection against malicious content attempting to enter the network data stream.

IPSs also protect against rate-based attacks such as DDoS attacks. Such attacks, which attempt to flood a network with seemingly legitimate traffic in order to overwhelm it, are often perpetrated for financial gain — hackers will threaten an organization with a DDoS attack unless a ransom is paid. IPSs block rate-based attacks through advanced techniques that distinguish legitimate from seemingly legitimate traffic.

"Intrusion protection systems not only protect against unauthorized access and malicious content that exposes sensitive data, but also stop rate-based attacks



that can be used for extortion purposes," said Reed. "As a result, IPS technology plays a key role in meeting business risk mitigation requirements."

## Legal Mandate

Protection against DDoS attacks in particular is vital given today's regulatory climate. Government regulations such as HIPAA, the Gramm-Leach Bliley Act (GLBA) and Sarbanes Oxley (SOX), as well as industry regulations such as the Payment Card Industry (PCI) Data Security Standard (DSS) continue to drive security purchases. While these regulations are concerned primarily with the confidentiality, integrity, security and availability of sensitive information, compliance extends to protection against DDoS attacks.

"The intent of regulations such as Sarbanes-Oxley and GLBA is to ensure against external threats to an organization's network," said Reed. "DDoS attacks are a real threat to the integrity and secure availability of confidential sensitive data."

IDSs are effective at preventing these kinds of attacks but they're not a panacea. Experts recommend a layered defense that includes perimeter firewalls, e-mail gateway scanning, desktop anti-virus protection and other security components. However, like a sentry posted at the castle gate, IPSs can not only detect attacks but prevent intruders from gaining access to the network.

## The Sentinel

Copyright © 2008 CMS Special Interest Publications. All rights reserved.

Editorial Correspondence:

4941 S. 78th E. Ave.,

Tulsa, OK 74145

Phone (800) 726-7667

Fax (918) 270-7134

Change of Address: Send updated address label information to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission. The Sentinel is published bimonthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

# Who's Accessing Your Network?

**Protect your wireless, wired  
and VPN networks with  
advanced network access  
control solutions from  
Bradford Networks.**



Bradford's NAC solutions deliver comprehensive identity management, endpoint compliance assessment, and usage policy enforcement capabilities that minimize the potential for security threats getting into the network. Bradford's patent-pending, award-winning, out-of-band appliances leverage existing network infrastructure to automatically enforce NAC policy at the network edge, making networks more secure and efficient.

**NAC Director™** delivers a complete NAC solution to enterprise customers in a variety of industries.

**NAC Director Guest/Contractor Services (GCS)** expands upon the flagship NAC Director solution to provide flexible and secure access to visiting users on an enterprise's network.

**Campus Manager** delivers comprehensive NAC to educational institutions.

**Contact your Classic Networking representative today to learn more about NAC solutions.**