



INTERNET  
SECURITY  
SYSTEMS™

**Active Wireless Protection**

*(September 2002)*

## Introduction

Wireless networks based on the 802.11b (WiFi) and similar standards are convenient, inexpensive and easily deployed without great technical expertise. As such, they are rapidly finding a home within home and enterprise networks. The advantages and cost savings introduced by wireless mobility also create significant security risks. This white paper explains a proactive methodology that enables organizations to safely and securely control and manage WiFi networks within a business environment.

## Technology Components

The start of any cycle of improvement begins with Vulnerability Assessment (VA). VA establishes a feedback loop that enables a company to measure their improvement and adjust their policy and configuration to continue to improve their security. There are several required VA components needed for wireless protection.

**Wireless Scanner** – The **Wireless Scanner**™ application discovers rogue Access Points and identifies some 802.11 protocol specific security issues. While Wireless Scanner is an excellent starting point for discovering access and protocol weaknesses, its sole use misses a significant piece of securing wireless. The majority of the security risk coming over 802.11 is still going to be TCP/IP vulnerabilities and threats.

**Internet Scanner** – The **Internet Scanner**® application identifies the majority of all TCP/IP issues and security risks, including Denial of Service attacks, buffer overflows, backdoors, Trojan Horse programs, misconfigurations, and popular hacker techniques.

**System Scanner** – The **System Scanner**™ application identifies security holes on specific servers that are connected to the wireless network. System Scanner finds internal vulnerabilities on a host, identifies many missing patches, and alerts users as to whether files are being modified to include backdoors and Trojan Horse programs.

**Database Scanner** – Many wireless applications connect to a relational database. The **Database Scanner**® application helps secure the database against vulnerabilities is not only important for safeguarding its data, but also prevents attackers from compromising other parts of the network using the database server.

VA identifies not only where there are vulnerabilities, but also helps identify where to apply Protection Agents. Protection Agents immediately detect and prevent threats that could compromise a computer network. Protection Agents need to be applied at the wireless clients (laptops and desktops), at the back-end servers for wireless, and behind the Access Points to defend the wired network from the wireless network. There are several Intrusion Protection System (IPS) components required for wireless protection.

**RealSecure Guard** – Put behind an Access Point, the **RealSecure**® **Guard** application stops and prevents most TCP/IP threats from originating from the wireless network against the wired network. RealSecure Guard prevents Denial of Service attacks, port and service probing, port scanning, buffer overflow attacks, and many other hacker techniques.

**RealSecure Server Sensor** – When the **RealSecure**® **Server Sensor** is installed on servers accessible via the wireless network, those servers become significantly hardened against wireless attacks.

**RealSecure Desktop Protector** – The **RealSecure**® **Desktop Protector** agent provides any laptop or desktop installed as a wireless client with comprehensive protection against attack or misuse, even when they are not connected to the corporate network – including mobile protection for remote, travel or home use.

There are two responsible approaches to Wireless IDS protection:

- **Wireless Scanner Discovery mode** – If a company wants to monitor 802.11 specific attacks, Wireless Scanner features a discovery mode. In discovery mode, Wireless Scanner sends alarms and events when an attacker tries to brute force the Access Point. Wireless Scanner specifically looks for attacks against the 802.11 authentication and encryption keys.
- **RealSecure Network Sensor Access Point alerts** – The other method is to look at the bigger area of risk. Most wireless attacks have to come through TCP/IP as the main attack vector. This area can be addressed by putting RealSecure Network Sensor behind the Access Point. This solution is very similar to RealSecure Guard, except it only alerts and does not prevent the attacks.

The VA, intrusion detection system (IDS), and IPS components all need to be configured by a single management product. One of the most important values to bringing all these components together is the correlation and analysis that provides the simple formula of:

#### **Risk = Vulnerabilities x Threats x Asset Values**

The **RealSecure® SiteProtector™** management console, especially with the security fusion module installed, performs the difficult task of correlating vulnerabilities and threats together under one management system. This dramatically reduces the number of events by only focusing on wireless attacks against wireless vulnerabilities. When many IDS technologies run as stand-alone applications, they ignore that most events are against protected hosts, and that a security operator wastes a tremendous amount of time investigating all these false alarms. Security fusion saves time, money, and focuses resources on the critical events.

SiteProtector embodies the Risk formula for bringing together vulnerabilities, threats, and asset values to enable a customer to understand their risk.

Bringing together the management, fusion, IDS, IPS, and VA components into a single integrated system provides active protection for wireless networks.

#### **Service Components**

Many forms of service components are layered on top of the active protection platform. A trusted security advisor should provide these service components, including:

- **Strategy, Policy, and Architecture Workshops for Wireless Security** – Educates and gets customers to think through policy issues, strategy, and how the architecture for the wireless security should be designed.
- **Security Assessments and Penetration Tests for Wireless Security** – Validates security issues associated with the current wireless network and helps form corrective action to eliminate vulnerabilities and security gaps in the policy.
- **Deployment of Active Protection Solution for Wireless Security** – Uses the proper methodology for the best optimized solution tailored to the environment and puts the best practice process in place. This component is key to the success of properly protecting the wireless environment.
- **Monitoring of Intrusion Detection around Wireless** – Managed Security Services offers 24/7 monitoring of IDS sensors and can be configured to identify attacks coming from wireless networks.

- **Emergency Response Services for Wireless Networks** – When a compromise does happen, it is useful to engage a very experienced team who understands security forensics and knows how to implement an effective incident response plan.
- **24/7 Technical Support for Wireless Protection Solution** – If there is a technical issue at any time, it is important to reach technical support to get quick and effective answers.

## Conclusion

WiFi networks are here to stay. Secure utilization of WiFi technology requires a multilayer approach that integrates vulnerability assessment and IDS into a robust, closed loop security management strategy. Internet Security Systems' Wireless Scanner, Internet Scanner, System Scanner, Database Scanner and RealSecure already provide significant protection for WiFi deployment, and can be utilized as part of a wireless IDS grid. This new area of information protection will undoubtedly continue to grow, and Internet Security Systems' X-Force will continue to provide secure wireless advice as this process evolves.

## Appendix – Wireless IDS with Existing Internet Security Systems Solutions

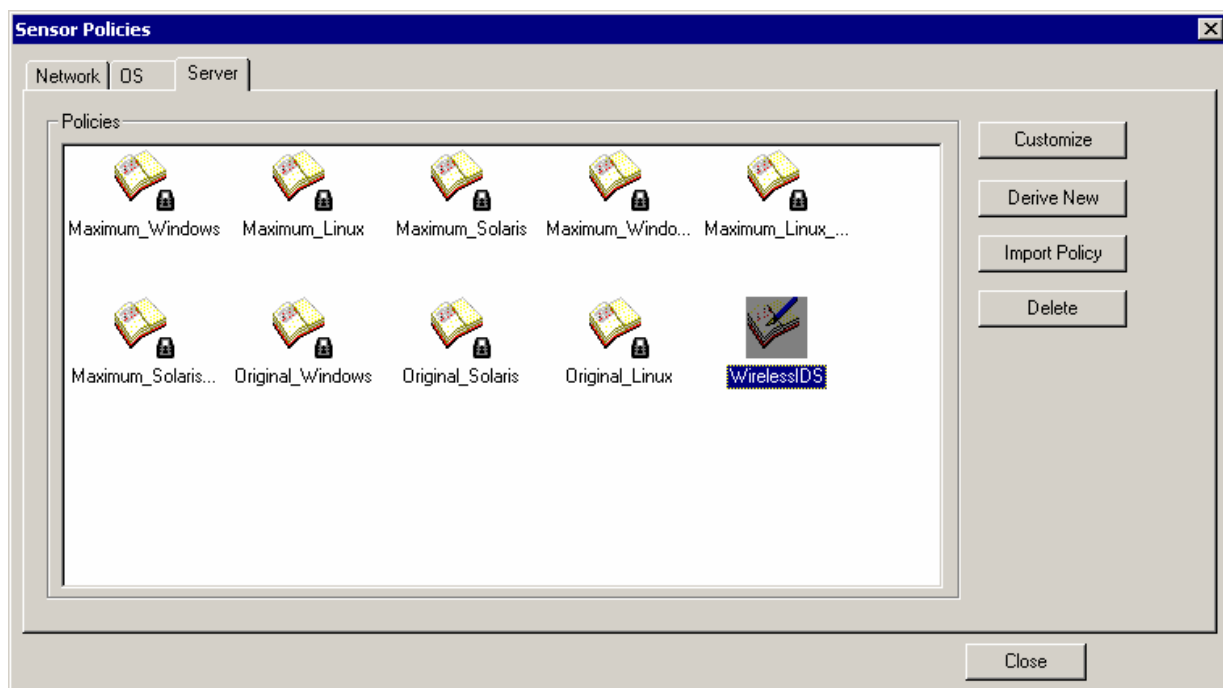
This example of wireless IDS is a consolidation of RealSecure Server Sensor and Wireless Scanner products running on the same system. It is not supported by Internet Security Systems' Customer Support organization, and should be implemented by security administrators or a security professional services consultant.

The first step is to deploy a workstation/laptop that has Wireless Scanner and a RealSecure Server Sensor installed. The Wireless Scanner is set to run continuously (24/7) and will log any suspicious wireless activity. The Server Sensor is configured to monitor this log and alert if any Access Point (AP) or Wireless client is activated. The Wireless IDS can even alert if an existing AP's configuration becomes insecure (e.g. WEP is disabled). This ensures that someone isn't altering an authorized wireless device within the boundaries an organization's network.

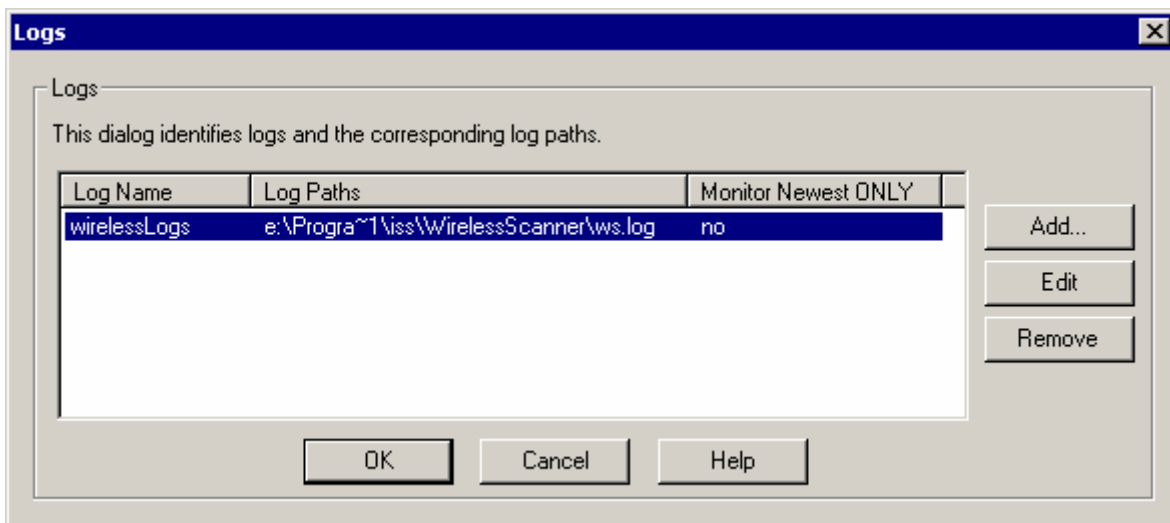
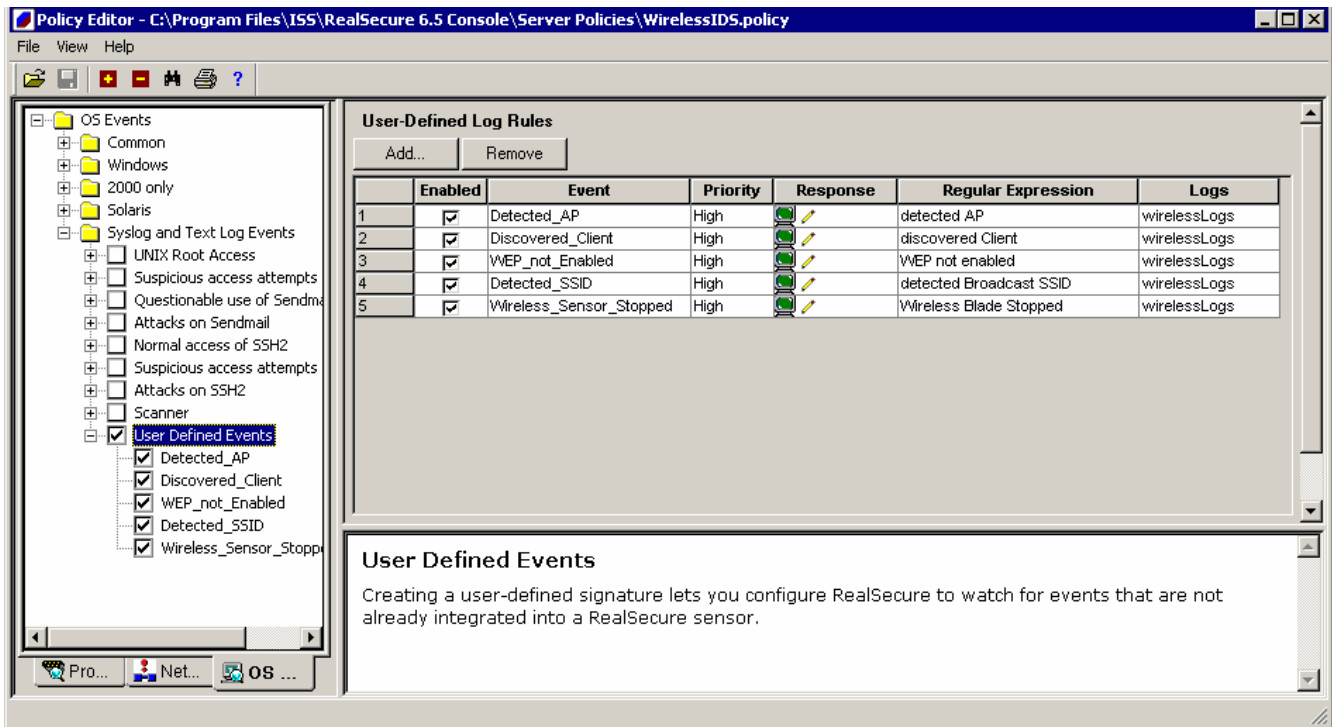
The alerts can be configured for pager, email, sent SNMP traps, alarm sounds, alerts to the RealSecure console, etc. This will happen in real time to minimize delays between wireless vulnerability assessment and remediation. Once everything is in place, the wireless IDS grid enables "wireless free" areas within corporate networks, and generates instant alerts should this change. Another advantage is that wireless IDS can be deployed in a stealth manner to hide the presence of the wireless IDS from attackers. Internet Security Systems' technology utilizes a dedicated driver, enabling a "listen only" mode, making the wireless IDS difficult to discover.

### How to configure

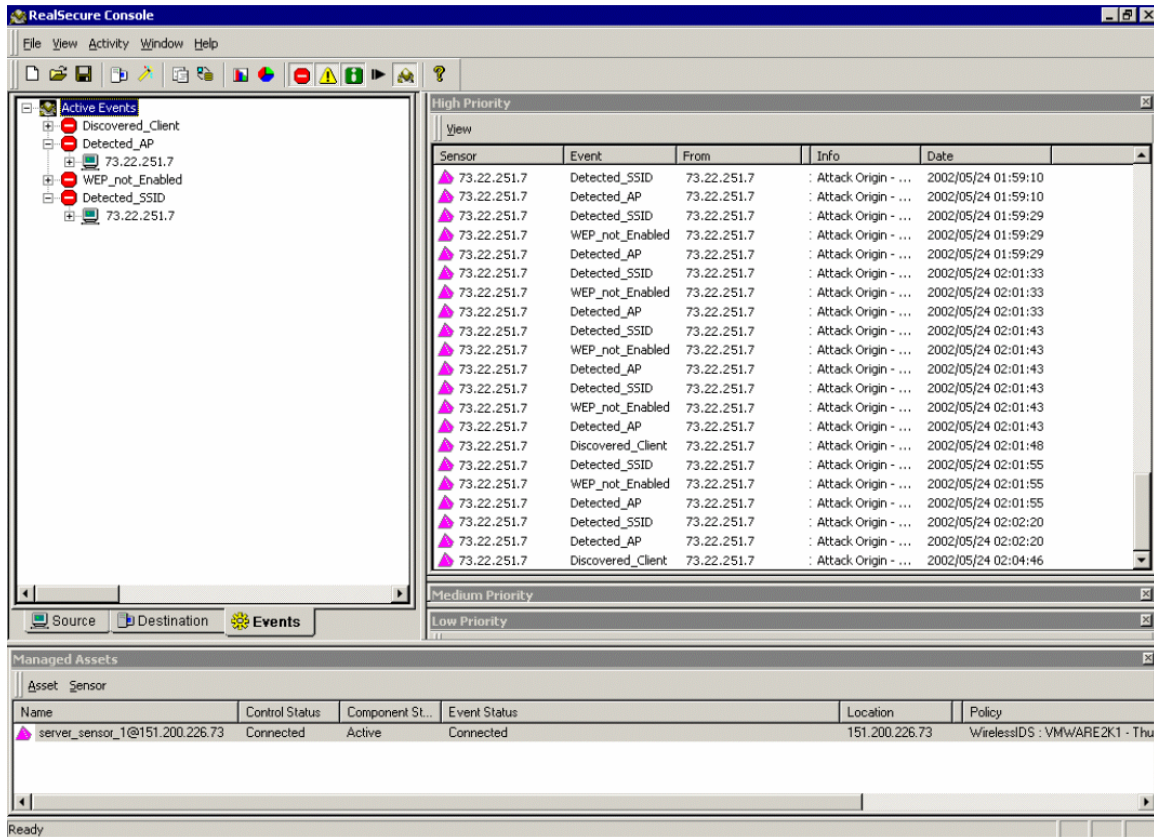
1. Install Wireless Scanner onto a system with a supported Wireless network card and a standard network card connected to your network.
2. Configure Wireless Scanner to start a Live Data scan and use the DiscoveryOnly policy.
3. Install RealSecure Server Sensor without network monitoring and establish communications with the RealSecure management console.
4. In the RealSecure management console, derive a Server Sensor new policy and name it WirelessIDS – see diagram below.



5. Customize this policy and add the following User Defined Events under the “Syslog and Text Log Events” section.
  - a. Detected\_AP
  - b. Discovered\_Client
  - c. WEP\_not\_Enabled
  - d. Detected\_SSID
  - e. Wireless\_Sensor\_Stopped
  
6. Each User Defined Event will use the event name as the Regular Expression and use the following log file <drive name>:\Progra~1\iss\WirelessScanner\ws.log. You must use the shortened “\Progra~1\” so that Server Sensor can correctly find the log file.



7. Start the Wireless Scanner and test the detection of Wireless devices.
8. You should start to see events in the RealSecure management console when a Wireless device is brought into range of the Wireless IDS sensor.



You now have a Wireless IDS protection sensor that can be deployed in areas where you wish to be alerted the moment a Wireless device is brought into the area.

**About Internet Security Systems (ISS)**

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a pioneer and world leader in software and services that protect corporate and personal information from an ever-changing spectrum of online threats and misuse. Internet Security Systems is headquartered in Atlanta, GA, with additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at [www.iss.net](http://www.iss.net) or call 888-901-7477.

*Copyright © 2002, Internet Security Systems, Inc. All rights reserved worldwide.*

*Internet Security Systems, the Internet Security Systems logo, System Scanner, Wireless Scanner, and SiteProtector are trademarks, and SAFEsuite, RealSecure, Internet Scanner and Database Scanner registered trademarks, of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.*