Cisco Adaptive Wireless Intrusion Prevention System: Protecting Information in Motion

What You Will Learn

The wireless spectrum is a new frontier for many IT organizations. Like any other networking medium, wireless spectrum must be properly secured, even if wireless networking is not deployed on site.

The Cisco® Adaptive Wireless Intrusion Prevention System (IPS) is integrated in the Cisco Unified Wireless Network infrastructure and provides wireless-specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption. Cisco Adaptive Wireless IPS provides the ability to visualize, analyze, and identify wireless threats, and centrally manages mitigation and resolution of security and performance issues. Cisco Adaptive Wireless IPS also delivers proactive threat prevention capabilities for a hardened wireless network core that is impenetrable by most wireless attacks.

Business Challenge

The growth of wireless networking and the sheer number of new mobile computing devices has blurred the traditional boundaries between trusted and untrusted networks, and shifted security priorities from the network perimeter to information protection and user security. The need to secure information in motion and control the wireless environment to prevent unauthorized access must be a priority for maintaining the integrity of corporate information and systems. The need to secure the airwaves applies to both companies with wireless networking installed and to companies that want to ensure no unauthorized wireless is in use.

In 2007, the National Cyber Security Alliance and Cisco polled companies using wireless networking and found that 67 percent either don't know their wireless security policies or have poor and outdated wireless security methods, and only 52 percent of enterprises surveyed regularly scanned their RF environment. Without proper wireless threat prevention, customer networks are vulnerable to:

- Rogue wireless access points that can be innocently introduced by well-meaning staff or by outsiders with malicious intent, but in either case create backdoor access to the company's network. This is a concern for both companies with wireless networking deployed and for companies without wireless networking.
- A wide variety of Wi-Fi-enabled clients that can also create backdoor access to the company's network.
- Hacker access points that try to lure users into connecting to them for purposes of network profiling or stealing proprietary information.
- Denial of service that disrupts or disables your wireless network.
- Over-the-air network reconnaissance, eavesdropping, and traffic cracking.
- Security vulnerabilities from non-802.11 wireless devices such as Bluetooth, which as it becomes more available and powerful, can present a significant threat.

The RF spectrum within the company perimeter is a business asset that must be managed and secured for the benefit of the business. Hackers, once motivated only by fame and notoriety are now more likely to be part ofinternational criminal enterprises that are constantly developing new methods of attack to acquire financial and confidential information. Recently, there have been highly publicized cases in which companies that neglected to secure their RF environment have found their customer financial data exploited by hackers; these companies were publicly criticized and forced to pay large fines. In fact, the costs associated with a security breach of customer or financial data can include the following:

- Regulatory fines
- Cost of third-party security audits
- Compensation to customers or partners
- Loss of customer confidence resulting in a decrease in future revenues
- Damage to the corporate brand
- Drop in market capitalization

Mobility creates a unique dichotomy for IT managers. Mobility demands more open networks and freedom of access to corporate information, which conflicts with many security policies that demand less access and more control. What's more, many administrators wind up using a variety of tools to protect their networks. Unfortunately, these tools often provide a disjointed view of security threats that make it impossible to correlate events and diagnose attacks.

While these is a lot to consider in wireless security, the good news is that all of these concerns are addressed by security technologies built-in to the wireless controllers, access points, mobility services engine, and wireless control system (WCS) that comprise the Cisco Unified Wireless Network infrastructure. So the same wireless equipment that provides connectivity to your users also provides security for the entire deployment.

Benefits of Secure Mobility

To help business provide secure wireless access, Cisco has taken all of the components required for a secure wireless deployment and purpose-built them into the Unified Wireless Network infrastructure. Using the same infrastructure to deliver network services as well as advanced security, Cisco provides comprehensive wireless security and intrusion prevention while reducing capital costs and streamlining security operations. Cisco provides a complete integrated solution

for wireless IPS without requiring separate single-purpose equipment, software, or management tools.

A network designed for proactive threat prevention is at the core of the Cisco Adaptive Wireless IPS solution. To identify unknown threats, wireless IPS has the ability to see in real-time both traffic and devices within the WLAN infrastructure, and to see them both on the wired networkand in the air. This increases detection and correlation capabilities as well as increasing threat detection accuracy and is much more effective than only monitoring the RF environment.

As an integral part of the Cisco Self-Defending Network, Cisco Adaptive Wireless IPS collaborates with Cisco's wired network security portfolio to provide a superset of networkwide threat protection for both the wired and wireless network. Furthermore, creating layered defenses delivers more thorough protection, greater accuracy, and operational efficiency for both network operations and security operations teams within IT departments.

The Cisco Adaptive Wireless IPS helps companies create secure networks that are capable of supporting proliferation of mobile devices and access to business applications in motion. The system also enables businesses to meet compliance requirements as set forth by the Payment Card Industry (PCI), the Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA), and other regulations. With Cisco Adaptive Wireless IPS, businesses can continue to realize the mobility opportunity with the confidence that critical business assets and information remain secure.

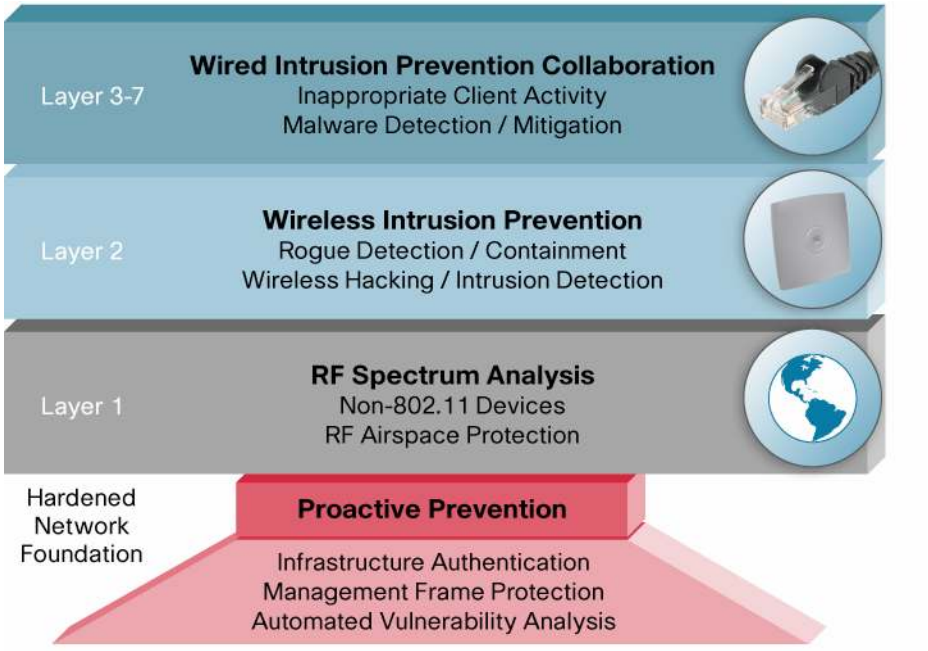
Comprehensive Threat Detection Coupled with Proactive Prevention and Wired Security Collaboration

Cisco unifies complete wireless threat detection and mitigation with the wireless and wired network infrastructure to deliver the industry's most comprehensive, accurate and operationally cost-effective wireless security solution. Building on this foundation are layers of RF intelligence, wireless intrusion prevention, and wired network security collaboration that protect against attacks that can originate anywhere from Layer 1(the physical frequency) through Layer 7 (the application layer).

Three components form the foundation of this uniquely comprehensive approach to wireless intrusion prevention:

- Network analysis and signature-based techniques integrated into the wireless infrastructure to deliver protection against rogue access points and clients, over-the-air wireless threats, zero-day attacks, performance degradation, and security configuration vulnerabilities. Continual threat research to develop new detection and mitigation techniques.
- Proactive threat prevention integrated in the wireless infrastructure that employs networkwide user and infrastructure authentication and encryption, wireless management frame protection, and automated wireless security vulnerability assessment and reporting to harden the wireless network core.
- Collaboration with the Cisco wired network security portfolio, providing a layered superset for wireless security protection.

Figure 1. Complete Protection: Cisco Wireless IPS Threat Detection Coupled with Proactive Prevention and Wired Security Collaboration



Comprehensive Wireless Threat Detection and Mitigation

Cisco Adaptive Wireless IPS is integrated directly into the Cisco Unified Wireless Network infrastructure. Taking advantage of standard Cisco wireless controllers, access points, the Cisco Mobility Services Engine and Wireless Control System for wireless threat detection and prevention reduces costs, streamlines operations, and provides comprehensive protection.

At the core of the Cisco Adaptive Wireless IPS is an advanced approach to wireless threat detection and performance management. While most market solutions rely solely on over-the-air passive traffic monitoring, Cisco Adaptive Wireless IPS combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention. Because the solution is infrastructure integrated, Cisco can continually monitor wireless traffic on both the wired and wireless network, and can use that network intelligence to analyze attacks from many different sources of information to more accurately pinpoint and proactively prevent attacks instead of waiting until damage or exposure has occurred.

Building upon the core detection capabilities, Cisco Adaptive Wireless IPS delivers rich attack classification as well as mitigation alerting, and reporting features. From a classification standpoint, the system provides users with flexible rules for automatically classifying security events. Automatic classification, coupled with the system's inherent accuracy, greatly reduces the operational expenses associated with manual investigation of potential threats detected by the system. The classification can also be linked with the threat mitigation actions, enabling either manual or automatic mitigation of security events based on their severity. Furthermore, based on the severity classification of the event, the system can alert IT operators of both detection and mitigation events.

To assure full visibility into the wireless environment, Cisco Adaptive Wireless IPS also detects performance-related issues and non-802.11 devices (Bluetooth, radar, microwaves, etc.) and attacks. Utilizing radio resource management (RRM), the system provides unmatched performance and network self-healing. Information collected pertaining to noise and interference, as well as client signal strength and other data, are used to dynamically assign channels and

adjust access point transmit power in real time to avoid co-channel interference, route around failed devices, and minimize coverage holes. For performance degradation and attacks spawned by non-802.11 sources, the solution delivers an RF spectrum expert with the ability to detect non-802.11 devices or sources of interference that could mask denial-of-service attacks generated by non-802.11 devices. Non-802.11 devices such as Bluetooth access points can impact performance of wireless networks, or even more damaging, create ad hoc connections to your wireless network through authenticated client devices.

Cisco Wireless Control System (WCS) provides wireless IPS network management and reporting on a unified configuration as well as security event management and reporting with physical location tracking of where the security event took place on the network. With system forensics, an administrator can actually play back events with the ability to trace, locate, and capture any WLAN or RF event. Real-time security posture and events are viewed via a consolidated security dashboard in WCS. Historical event data can be stored using the Mobility Services Engine as a platform, allowing for access to large files with multiyear, forensic data reporting accessible via WCS. This can allow for more complex analysis over time as well as compliance reporting.

Hardened Network Core with Proactive Threat Prevention

The best way to secure your network is to design a system that prevents an attack before damage can be done. The Cisco wireless IPS solution is built upon a hardened wireless infrastructure that uses networkwide user and infrastructure authentication and encryption, taking advantage of IEEE 802.11i and 802.1X, Cisco's wireless management frame protection (MFP), and automated wireless security vulnerability assessment and reporting. Additionally, constant monitoring of wireless client activity prevents out-of-policy or malicious clients from accessing the network.

Requiring a valid 801.1X wired port authentication for Cisco Aironet® access points to connect to a wired port essentially eliminates the possibility that a rogue access point will join the wired network. Advanced encryption provides protection for data in transit and management frame protection (the basis for the IEEE 802.11w standard) renders most wireless attacks ineffective by protecting 802.11 management frames traversing the air. In conjunction with strong authentication, MFP proactively prevents most over-the-air wireless attacks while increasing the fidelity of rogue access point detection via use of over-the-air digital signatures, which renders over-the-air reconnaissance fruitless.

The wireless network automatically performs automated 24/7 wireless vulnerability monitoring and assessment by proactively and persistently scanning the wireless network for weak security configurations. Understanding the security posture of the wireless network in real time is the most important aspect of attack prevention.

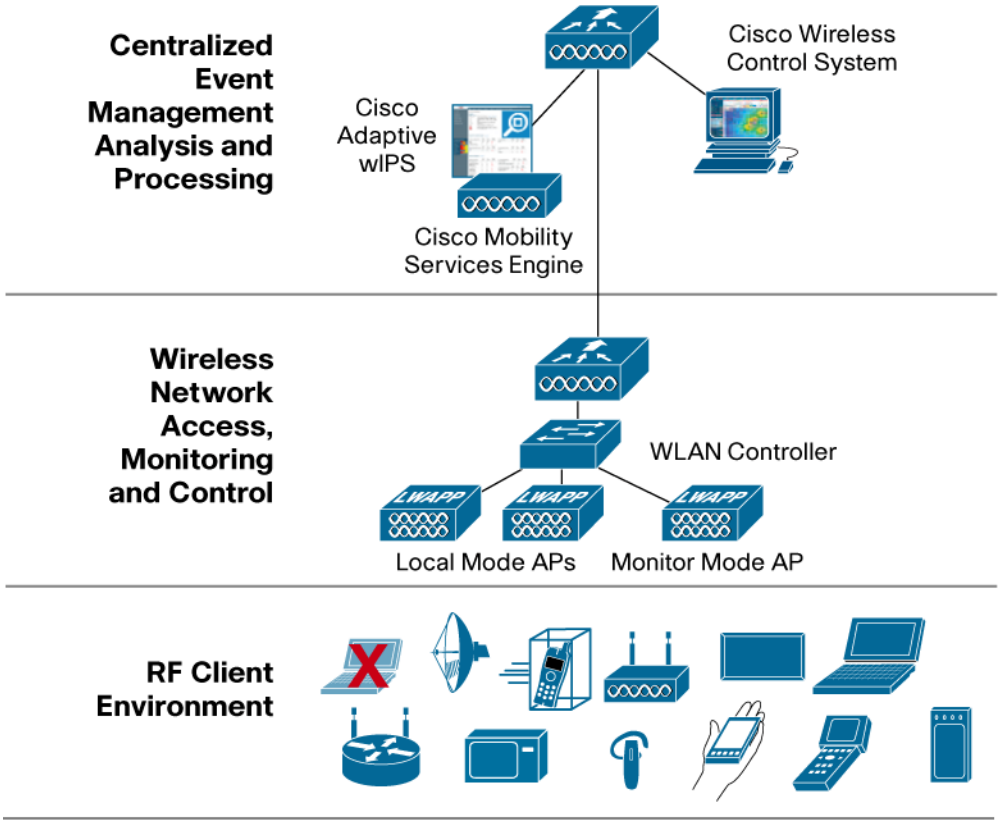
The Components Used to Deploy Cisco Adaptive Wireless IPS

All the components required for secure deployment and operations of a wireless network infrastructure are built into the Cisco Unified Wireless Network. The Adaptive Wireless IPS system is composed of the following CUWN components, (also outlined in the network diagram below):

- Cisco Mobility Services Engine with Cisco Adaptive Wireless IPS
- Cisco Aironet Access Points
- Cisco WLAN Controllers and Wireless Control System

Using the Cisco Mobility Services Engine within the Cisco Unified Wireless Network, Cisco Adaptive Wireless IPS scales to meet the robust demands of even the largest networks. Continuous 24 x 7 monitoring is performed by Cisco Aironet access points which feed back information to the centralized processing platform within the Mobility Services Engine. In this way, Cisco is able to efficiently collect and correlate wireless traffic analysis and security status from all reaches of the network to provide a simple, unified view into the security state of the wireless network.

Figure 2. Components of the Cisco Adaptive Wireless IPS Solution



The Cisco Mobility Services Engine provides analysis processing performance and scalability, storage capacity for historical reporting and forensics, and integration capabilities for services such as location or contact aware asset tracking and client security management. As the mobile business network expands, the Cisco Adaptive Wireless IPS solution provides monitoring and analysis of the growing number of new devices and spectrum uses to ensure ongoing protection of critical business information.

Cisco can supply wireless IPS scanning from Cisco access points simultaneously servicing user traffic or the access points can be configured for full-time dedicated wireless IPS monitoring. Providing both shared and dedicated monitoring options enables flexibility to meet site-specific deployment requirements. In local mode, Cisco access points spend part of their time servicing data to wireless clients and part of their time performing wIPS scanning. While in monitor mode, the access point performs wIPS scanning full-time. Part-time local mode and full-time monitor mode access points can be mixed to satisfy the overall network architecture requirements.

The Wireless Control System (WCS) provides centralized planning, configuration, management and reporting that allows IT managers to design, control and monitor hundreds of Cisco Wireless

LAN Controllers and thousands of access points over wide geographies from a single console, simplify operations and reducing total cost of ownership. For ease of use and to provide wireless LAN administrators confidence in WLAN security settings, WCS provides a robust graphical user interface, policy templates and vulnerability scanning with recommended mitigation based on Cisco best-practices to assist administrators in wireless LAN security configuration, monitoring and administration. WCS also provides network wide reporting capabilities, including a unified dashboard for all security events and compliance reporting such as the PCI Assessment Report. WCS is a management tool for all wireless and wireless security operations that simplifies workflows, reduces time spent training operations staff, and reduces software costs.

Enhancing Wireless Security via Collaboration with Wired Network Security

The Adaptive Wireless IPS system can collaborate with the Cisco wired network security portfolio, providing a superset wireless security protection. Collaboration with the wired network offers protection against malware, consistent client security posture enforcement and unified wired/wireless security monitoring across the network. This provides a layered approach to wireless security.

For example, Cisco wireless IPS and wired IPS platforms can collaborate in real-time to disconnect a wireless user spreading a virus or worm. Cisco Network Admission Control can enforce wireless client security posture. And the ability to send all wireless security events from the Cisco wireless IPS to the Cisco MARS security information management system provides a network-wide view and analysis of both wired and wireless security. Creating a common platform for your wired and wireless network provides layered defenses which deliver more thorough protection, with greater accuracy and operational efficiency for both network operations and security operations teams within IT departments.

Unlike conventional tools, the Cisco Adaptive Wireless IPS solution provides a holistic threat prevention system designed to provide proactive protection and the only true threat suppression capability across wired and wireless networks.

Why Cisco?

The Cisco® Unified Wireless Network allows businesses to implement mobility applications across disparate networks. The barriers between personal, private, and public networks disappear, delivering a secure and consistent mobility experience. When you deploy a Cisco Unified Wireless Network, our technology expertise and deployment experience, combined with Cisco partner solutions, help your company to benefit from a high-performing, flexible, and scalable wireless infrastructure.

Cisco empowers IT to meet and exceed business mobility demands of their employees and assets by:

- Providing collaborative security over disparate networks
- Proactively preventing threats associated with the increasing quantity and diversity of mobile devices
- Delivering device-to-network-to-application integration and security
- Creating a secure open platform for the development of mobility applications

Cisco Services and the wireless LAN specialized partners provide services to support a new, practical approach to business mobility that empowers corporations to meet their technology and

business objectives. The blueprint that Cisco provides unifies the mobility network, secures and manages mobile devices, and creates an open ecosystem for mobility applications. This is enabled by building an integrated platform by planning, deploying, and managing mobility solutions with far greater efficiency and allows greatly expanded capabilities in the areas of wireless client management, context aware solution services, and fixed-mobile convergence through end-to-end management and provisioning of services to enhance mobility of applications and protect your investment.

Cisco Services make networks, applications, and the people who use them work better together. To learn more about how Cisco and our global network of highly skilled wireless LAN specialized partners can help you increase the accuracy, speed, and efficiency of deploying or migrating to a centralized Cisco Unified Wireless Networking solution, visit http://www.cisco.com/go/wirelesslanservices or contact your local account representative.

For More Information:

For more information about Cisco Adaptive Wireless Intrusion Prevention Solution, visit: http://www.cisco.com/go/wips

For more information about the Cisco Self-Defending Network: http://www.cisco.com/go/sdn

For more information about the Cisco Mobility Services Engine, visit: http://www.cisco.com/go/mse

For more information about the Cisco Unified Wireless Network, visit: http://www.cisco.com/go/wireless

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-478925-00 05/08