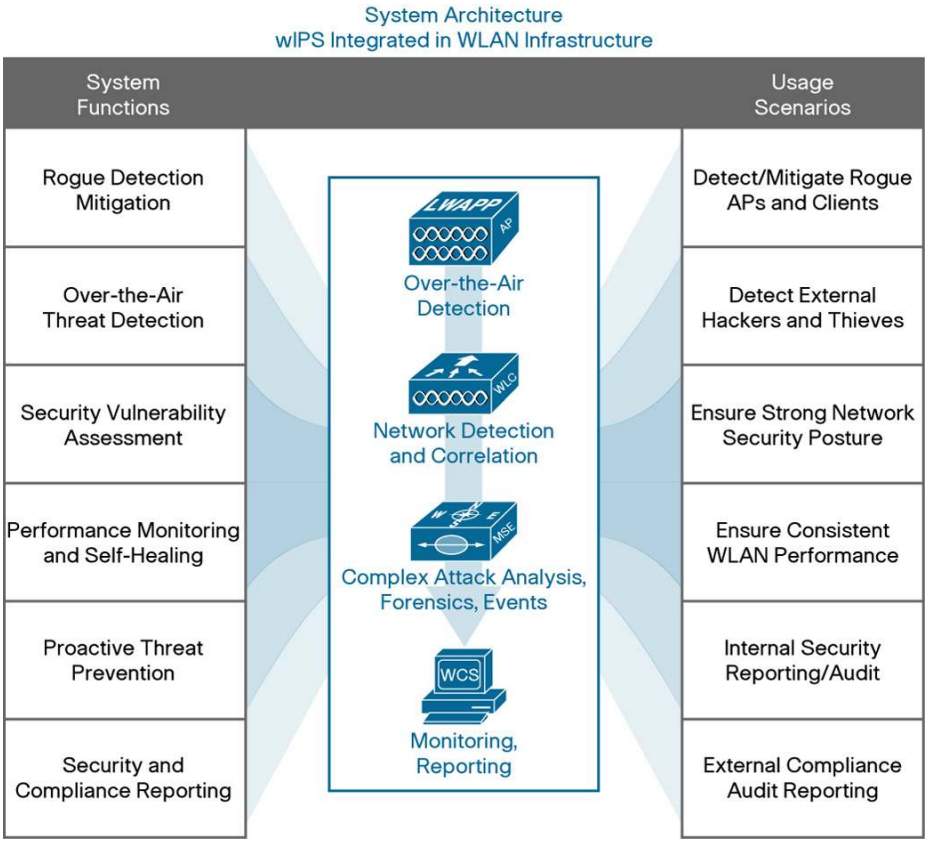
# Cisco Adaptive Wireless Intrusion Prevention System

## Product Overview

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

Cisco® Adaptive Wireless IPS (wIPS) 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 wIPS (Figure 1) provides the ability to detect, analyze, and identify wireless threats, and centrally manages mitigation and resolution of security and performance issues. Cisco Adaptive wIPS also delivers proactive threat prevention capabilities for a hardened wireless network core that is impenetrable by most wireless attacks, allowing customers to maintain constant awareness of their RF environment to minimize legal liability, protect brand reputation, and assure regulatory compliance - including PCI 2.0 standards.

**Figure 1.** Cisco Adaptive wIPS: System Overview



## Feature Overview

Cisco Adaptive wIPS embeds complete wireless threat detection and mitigation into the wireless network infrastructure to deliver the industry's most comprehensive, accurate, and operationally cost-effective wireless security solution. Adaptive wIPS performs: rogue access point/client and ad hoc connection detection and mitigation, over-the-air wireless hacking and threat detection, security vulnerability monitoring, performance monitoring and self-optimization, network hardening for proactive prevention of threats, and complete wireless security management and reporting.

## The Power of Integration in the Wireless Network Infrastructure

Cisco Adaptive wIPS is integrated directly into infrastructure components of the Cisco Unified Wireless Network, including Cisco wireless LAN controllers, Cisco access points, the Cisco Mobility Services Engine (MSE), and the Cisco Prime™ Network Control System (NCS). This integrated wireless threat detection and prevention reduces costs, streamlines operations, and provides comprehensive protection.

Integration of wireless IPS into the WLAN infrastructure offers more than just the cost and operational efficiencies delivered by using a single infrastructure for both wireless IPS and WLAN services. Integration enables a superset of capabilities not architecturally possible with standalone, overlay wireless IPS systems. New functionality delivered by the infrastructure-integrated architecture of Cisco Adaptive wIPS allows network administrators to:

- **See the whole picture:** Typical wIPS solutions rely solely on RF air monitoring for detection. Cisco Adaptive wIPS builds on RF air monitoring by employing network traffic and anomaly analysis within the access points and WLAN controllers, as well as real-time device inventory analysis and network configuration analysis to detect threats and monitor performance. This approach delivers more accurate and thorough detection.
- **Take corrective action:** Cisco Adaptive wIPS doesn't just detect threats, vulnerabilities and performance issues; it makes it possible to take corrective action. Integration in the WLAN infrastructure enables Adaptive wIPS to go beyond passive monitoring and reach into the infrastructure to fix security threats and performance issues, and to do so in real time.
- **Take advantage of the entire WLAN footprint:** Cisco Adaptive wIPS can use all the access points in the network for location and mitigation of rogue devices. This increases location accuracy and mitigation scalability.
- **Benefit from flexible deployment architectures:** Cisco Adaptive wIPS can use access points dedicated to full-time air monitoring or access points serving WLAN users. This deployment flexibility enables right-sized security models on a site-specific basis.

## Comprehensive Protection, Accurate Detection

Cisco's advanced approach to detection, combining air monitoring, network traffic and anomaly analysis, real-time network device and topology information, and network configuration analysis, delivers a comprehensive view of the event to the Cisco Adaptive wIPS analysis engine. With that breadth of information, Adaptive wIPS detects events not traceable with over-the-air signatures alone and makes more accurate detection decisions, thus increasing effectiveness while reducing false positives.

Building upon the core detection capabilities, Cisco Adaptive wIPS delivers rich attack classification, providing users with flexible rules for automatically classifying and mitigating 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.

Cisco couples these advanced detection and classification techniques with an extensive attack, vulnerability, and performance detection library. Examples of event classes detected include rogue access points/clients, ad hoc connections, hacker access points such as honeypots and evil twins, network reconnaissance, authentication and encryption cracking, man-in-the-middle attacks such as address/identity spoofing and replay attacks, protocol attacks, denial-of-service (DoS) attacks, over-the-air and network security vulnerabilities, and performance issues such as co-channel interference and coverage holes.

## Complementing Adaptive wIPS 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. Network security hardening features embedded in the Cisco Unified Wireless Network complement the Cisco Adaptive wIPS solution to provide the following proactive threat prevention techniques:

- **Remove security offenders from the network:** Client exclusion policies can automatically respond to high levels of user authentication failures and IP address spoofing.
- **Defuse network reconnaissance, spoofing, and man-in-the-middle attacks:** Cisco Management Frame Protection, the basis for IEEE 802.11w, encrypts and authenticates WLAN management frames to defend against many common over-the-air attacks.
- **Protect against data theft:** Strong user authentication and Wi-Fi Protected Access 2 (WPA2) and 802.11i encryption standards protect access to your network and data traversing the WLAN.
- **Lock out rogue access points:** Using 802.1X wired port authentication on Cisco access points virtually eliminates the possibility that a rogue access point will join the wired network.

## Features and Benefits: Technical Overview

The sections below outline each functional area of the Cisco Adaptive Wireless IPS solution and the associated benefits.

## Rogue Detection, Classification, and Mitigation

Cisco Adaptive wIPS features rogue detection and mitigation as shown in Table 1. Rogue access points and clients can create backdoor access to your network and can be used for data theft from your wireless clients. Adaptive wIPS detects, auto-classifies based on customizable rules, and mitigates rogue access points, rogue clients, spoofed clients, and client ad hoc connections.

**Table 1.** Features and Benefits: Rogue Detection, Classification, and Mitigation

| Feature | Benefit |
|---|---|
| **Detection** | |
| **On-/Off-Channel Scanning** | Detects rogue access points, rogue clients, spoofed clients, and client ad hoc connections on all channels in the 802.11-related spectrum |
| **Signature-Based and Network-Analysis-Based Detection** | Increases breadth and accuracy of rogue, ad hoc, and spoofing detection, thus decreasing manual threat investigation by staff |
| **Spectrum Intelligence** | Detects rogue devices and denial of service in non-802.11 frequencies, such as Bluetooth, radar, and microwave |

| Feature | Benefit |
|---|---|
| **Event Classification** | |
| **Customizable Rogue Event Auto-Classification** | Auto-classifies the threat level of rogue events-based user-defined classification rules, thus reducing staff intervention |
| **Rogue Switch-Port Tracing** | Establishes if a detected rogue access point is on the customer network, thus reducing manual staff investigation to assess the threat |
| **Physical Location of Rogue Device** | Plots rogue access points and clients on a floor map, thus helping assess the rogue threat and facilitate removal |
| **Mitigation** | |
| **Rogue Switch-Port Disable** | Remotely disables the Ethernet port to which a rogue access point is connected, thus speeding mitigation |
| **Over-the-Air Mitigation** | Mitigates rogue access points, clients, and ad hoc over-the-air connections using any Cisco access point deployed, thus speeding and scaling mitigation |
| **Automatic or Manual Mitigation** | Flexible mitigation actions enable tailoring to customer risk environment and operational model |

## Over-the-Air Attack Detection

Cisco Adaptive wIPS features over-the-air attack detection as shown in Table 2. Over-the-air attacks are launched by hackers adjacent to your RF environment. Since RF signals penetrate walls, an attacker could be someone sitting in the parking lot in front of your office. Attack types include network reconnaissance, authentication and encryption cracking, denial of service, and man-in-the-middle attacks, as well as impersonation attempts and new or unknown attack techniques.

**Table 2.** Features and Benefits: Over-the-Air Attack Detection

| Feature | Benefit |
|---|---|
| **Breadth of Attack Detection** | |
| **Network Reconnaissance and Profiling Detection** | Analyzes traffic behavior and performs pattern matching to detect tools and techniques such as Netstumbler, Wellenreiter, Kismet, honeypot access points, and other methods, providing an early alert that a hacker is looking for avenues of attack |
| **Authentication and Encryption Cracking Detection** | Analyzes traffic behavior and performs pattern matching to detect tools and techniques such as AirSnarf, AirCrack, ASLEAP, Chop-Chop, and other methods, providing an alert of potential or attempted data theft |
| **Malicious or Inadvertent Denial of Service Detection** | Analyzes traffic behavior and performs pattern matching to detect tools and techniques such as 802.11 protocol abuse, AirJack, RF jamming, resource starvation, and other methods, providing an alert of potential or attempted network service disruption |
| **Man-in-the-Middle Attack Detection** | Analyzes traffic behavior, performs pattern matching, and applies authentication methods to detect tools and techniques such as replay attacks, fake access points, 802.11 protocol manipulation, and other methods, providing an alert of potential data theft or unauthorized network access |
| **Impersonation and Spoofing Detection** | Analyzes traffic behavior, performs pattern matching, and applies authentication methods to detect tools and techniques such as MAC/IP spoofing, fake access points, evil-twin access points, Dynamic Host Configuration Protocol (DHCP) spoiling, and other methods, providing an alert of potential data theft or unauthorized network access |
| **Zero-Day Attack Detection** | Analyzes traffic behavior to detect newly introduced or previously uncategorized attack methods, providing an alert of a potential threat |
| **Ongoing Threat and Vulnerability Research and Detection Development** | Cisco has a wireless threat and vulnerability research team dedicated to finding out about new attack techniques, as well as proactively analyzing the network for vulnerabilities that could be exploited; the research team helps ensure that Cisco Adaptive wIPS detection capabilities stay ahead of the threat horizon |
| **Event Classification and Tuning** | |
| **Default Detection Profiles** | Default detection tuning profiles, customized by customer type, enable effective operation minutes after system startup and provide a head start in system tuning |
| **Knowledge-Base-Driven Tuning** | Detection tuning is tied to a threat knowledge base in NCS, giving operators plain-language descriptions of attack types and detection methods as well as tuning guidance, thus making tuning easier even for novice security operators |

## Security Vulnerability Monitoring

Cisco Adaptive wIPS features security vulnerability monitoring as shown in Table 3. Understanding the security posture of the wireless network in real time is the most important aspect of attack prevention. The Cisco NCS management system automatically performs automated 24/7 wireless vulnerability monitoring and assessment by proactively and persistently scanning the wireless network for weak security or out-of-policy configurations.

**Table 3.** Features and Benefits: Security Vulnerability Monitoring

| Feature | Benefit |
|---|---|
| **Automated, 24/7 Configuration Analysis** | Analyzes all wireless controller, access point, and management interface security configurations; by analyzing actual configurations rather than relying solely on over-the-air vulnerability sniffing, the NCS delivers greater accuracy and depth of vulnerability analysis, such as analysis of management protocol security and analysis of security services operating on the network |
| **Analyze Against Industry Best Practices or Customer-Specific Security Policies** | NCS is pre-populated with industry best practices for wireless security vulnerability assessment; using NCS Config Audit, customers can also analyze configurations against their own specific security policies; this dual approach enables the greatest flexibility and breadth of vulnerability analysis |
| **Broad Vulnerability Identification** | Identifies vulnerabilities that can result in unauthorized management and network access, data theft, man-in-the-middle attacks, DoS attacks, and protocol attacks, and advises on security services to run on the wireless network |

## Performance Monitoring and Auto-Optimization

Cisco Adaptive wIPS features performance monitoring as shown in Table 4. A poorly performing network affects network and application availability and can be a result of malicious or accidental means. Utilizing radio resource management (RRM), the system provides unmatched performance and network self-healing. Information about noise and interference, as well as client signal strength and other data, is used to dynamically assign channels and adjust access point transmit power in real time to avoid co-channel interference, to route around failed devices, and to minimize coverage holes.

**Table 4.** Features and Benefits: Performance Monitoring and Auto-Optimization

| Feature | Benefit |
|---|---|
| **Continuous Real-Time Monitoring of Network Health and Performance** | Defends against over-the-air interference, malicious or accidental |
| **Automatically Fixes Problems in the RF Domain** | Remedies issues, such as RF-based denial of service, without administrator intervention, thus increasing network uptime with minimal operational overhead |
| **Complete RF Management without Specialized RF Skills** | RF management expertise is into the system, thus reducing the burden on operational staff |

## Management, Monitoring, and Reporting

Cisco Adaptive wIPS features complete security management, monitoring, and reporting capabilities as shown Table 5. Adaptive wIPS management is fully integrated into the Cisco NCS, providing a single, unified tool for both wireless network and wireless security operations. Unification of wireless network and wireless security management reduces challenges by keeping access point and client device inventories and security policies aligned, and by simplifying event management and reporting.

**Table 5.** Features and Benefits: Management, Monitoring, and Reporting

| Feature | Benefit |
|---|---|
| **Single Management Platform for Wireless Network and Security** | |
| **Real-Time Device Inventories** | Access point and client device inventory is always up-to-date, with no double-entry or cross-vendor management integration issues, thus enabling high accuracy in rogue detection while minimizing administrative overhead |

| Feature | Benefit |
|---|---|
| **Virtualized Management Domains** | Adaptive wIPS enables split wireless security management and monitoring from other wireless management roles or geographies |
| **No One-Off Management Platforms** | All wIPS and general wireless management is performed from the NCS, thus minimizing staff training and support on disparate platforms |
| **Integrated with Cisco Unified Wireless Network Features** | wIPS provides unified workflows integrating general wireless network configuration, wireless security policy definition, and location service operation |
| **Command Authorization and Audit Trails** | All management commands can be authorized by authentication, authorization, and accounting (AAA); configuration, investigation, and mitigation actions logged can be traced back to the administrator, enabling accountability |
| **Designed for Enterprise Scalability** | The NCS is designed for the highest-scale environments: up to 3000 user-serving or wIPS access points per NCS instance |
| **NCS Security Dashboard** | |
| **Single, At-a-Glance View** | Single-screen summary of all security events and vulnerabilities presented in a streamlined, at-a-glance format; ability to drill down on classes of events and individual events with a mouse click; eases day-to-day monitoring |
| **Wired Security Integration** | Malware and hacking events associated with wireless users can be monitored from the NCS security dashboard, thus providing a network-wide view of wireless user activity |
| **NCS Performance (RRM) Dashboard** | |
| **Single, At-a-Glance View** | Single-screen summary of all performance-related events presented in a streamlined, at-a-glance format; ability to drill down on classes of events and individual events with a mouse click; eases day-to-day monitoring |
| **NCS Event Management and Reporting** | |
| **Complete Event Forensics** | Captures all traffic associated with an attack for ease of attack investigation |
| **Event Escalation to Staff** | Automatically alerts staff regarding critical events, thus decreasing response time; fully customizable by event type |
| **Per-Admin Reports** | Historical reports can be customized for individual administrators based on their preferences and area of responsibility, thus streamlining event analysis |
| **Report Auto-Scheduling** | Historical reports can be scheduled to run automatically at specific times, thus streamlining workflows |
| **Payment Card Industry (PCI) Reporting** | Historical reports may be customized for events pertinent to Payment Card Industry (PCI) compliance, thus streamlining audit-related activities |
| **Event Storage and Archiving** | Security attack events are stored in the Cisco Mobility Services Engine for long-term archiving, thus streamlining historical analysis |

## Adaptive Wireless IPS Software

### Monitor Mode

Cisco Adaptive WIPS Monitor Mode software licenses are based on the number of full-time monitoring access points that are deployed in the network. The Cisco 3355 Mobility Services Engine allows for the tracking of up to 3,000 monitoring access points, and the 3310 Mobility Services Engine allows for the tracking of up to 2,000 monitoring access points. The licenses are additive.

Monitor Mode SKUs:

- AIR-WIPS-AP-5: Supports 5 monitor mode Cisco access points
- AIR-WIPS-AP-25: Supports 25 monitor mode Cisco access points
- AIR-WIPS-AP-100: Supports 100 monitor mode Cisco access points
- AIR-WIPS-AP-500: Supports 500 monitor mode Cisco access points
- AIR-WIPS-AP-2000: Supports 2000 monitor mode Cisco access points

## Enhanced Local Mode

Cisco Adaptive wIPS Enhanced Local Mode software licenses are based on the number of local mode (data-serving) access points that are deployed in the network. The Cisco 3355 Mobility Services Engine allows for the tracking of up to 3000 local mode access points and the Cisco 3310 Mobility Services Engine allows for the tracking of up to 2000 local mode access points. The licenses are additive.

Enhanced Local Mode SKUs:

- AIR-LM-WIPS-5: Supports 5 enhanced local mode access points
- AIR-LM-WIPS-25: Supports 25 enhanced local mode access points
- AIR-LM-WIPS-100: Supports 100 enhanced local mode access points
- AIR-LM-WIPS-500: Supports 500 enhanced local mode access points
- AIR-LM-WIPS-2000: Supports 2000 enhanced local mode access points

The Cisco 3300 Series Mobility Services Engine supports coexistence of multiple mobility services on the same appliance. Both the 3310 and 3355 MSEs support Adaptive Wireless IPS and context-aware services on the same appliance.

## Standard Components of a Cisco Adaptive wIPS Are:

- All Cisco LWAPP access points are supported for Monitor Mode Adaptive wIPS monitoring
- All 11n LWAPP access points are supported for Enhanced Local Mode (ELM) wIPS monitoring
- Multiple mobility services can coexist with Cisco Adaptive wIPS on the same Mobility Services Engine (3310 and 3355)
- Up to 2000 wIPS access points can be served by a single 3310 MSE
- Up to 3000 wIPS access points can be served by a single 3355 MSE
- Requires Cisco WCS Version 5.2 or later for management, configuration, and reporting
- A Mobility Services Engine can be managed by a single NCS instance
- A single NCS instance can manage multiple Mobility Services Engines

## Licensing and Ordering Information

### Cisco Adaptive Wireless IPS Software

- Available with Cisco Mobility Services Engine Software Release 5.2.xxx or later
- Requires 5.2.xxx or later on Cisco Wireless Control System
- Requires 5.2.xxx or later on Cisco wireless LAN controllers
- Release 5.2 and later wireless IPS functionality requires Monitor Mode (that is, non-client-serving) access points
- Release 7.1.xxx and later wireless IPS functionality requires Enhanced Local Mode (that is, client-serving) access points

Cisco Adaptive wIPS is a licensed software feature set on the Cisco Mobility Services Engine. Table 6 shows the license levels available for Adaptive wIPS.

**Table 6.** Cisco Adaptive wIPS Software Licenses

| | |
|---|---|
| **Wireless IPS License, Supporting 5 Cisco Monitor Mode APs** | AIR-WIPS-AP-5 |
| **Wireless IPS License, Supporting 25 Cisco Monitor Mode APs** | AIR-WIPS-AP-25 |
| **Wireless IPS License, Supporting 100 Cisco Monitor Mode APs** | AIR-WIPS-AP-100 |
| **Wireless IPS License, Supporting 500 Cisco Monitor Mode APs** | AIR-WIPS-AP-500 |
| **Wireless IPS License, Supporting 2000 Cisco Monitor Mode APs** | AIR-WIPS-AP-2000 |
| **Wireless IPS License, Supporting 5 Enhanced Local Mode APs** | AIR-LM-WIPS-5 |
| **Wireless IPS License, Supporting 25 Enhanced Local Mode APs** | AIR-LM-WIPS-25 |
| **Wireless IPS License, Supporting 100 Enhanced Local Mode APs** | AIR-LM-WIPS-100 |
| **Wireless IPS License, Supporting 500 Enhanced Local Mode APs** | AIR-LM-WIPS-500 |
| **Wireless IPS License, Supporting 2000 Enhanced Local Mode Apes** | AIR-LM-WIPS-2000 |

## Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, visit Cisco Technical Support Services or Cisco Advanced Services.

## For More Information

For more information about Cisco Adaptive wIPS, visit http://www.cisco.com/go/wips.

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 C78-501388-03 10/11