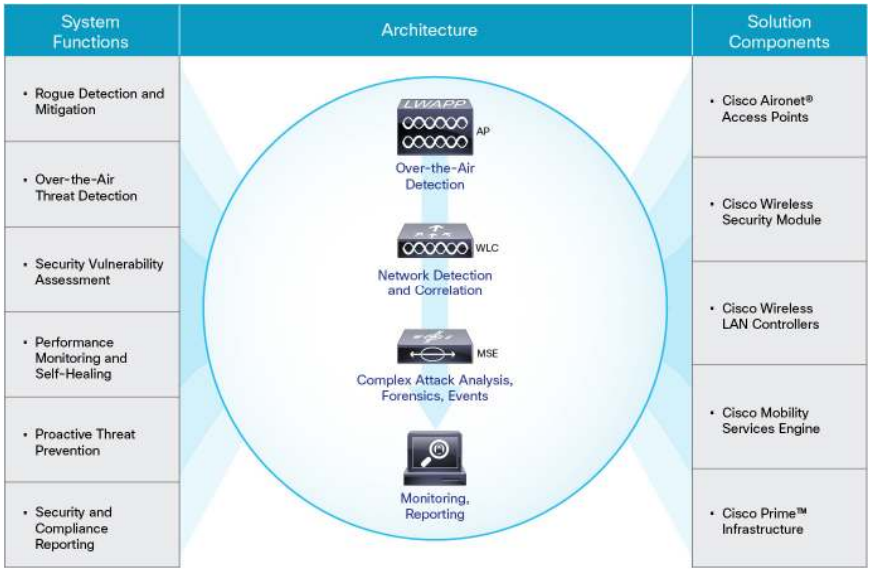
Cisco Wireless Intrusion Prevention System

Solution Overview

Ten billion. That's how many mobile devices will populate our planet by 2017. [1]This rapid proliferation in mobility is increasing the need for wireless connectivity. Many organizations are responding to this trend by providing Wi-Fi access to employees and guests, which presents many opportunities but also poses new threats to the network. Savvy mobile users can set up wireless networks just by using their smartphones - providing connectivity for the user but also a potential entry point for an intruder. Hackers continue to target vulnerable wireless networks with constantly changing threats, so IT organizations are constantly challenged to both track and locate wireless threats throughout the organization and demonstrate compliance.

Figure 1. Cisco Adaptive wIPS: System Overview



Cisco® Wireless Intrusion Prevention System (wIPS) is a complete wireless security solution that uses the Cisco Unified Access™ infrastructure to detect, locate, mitigate, and contain wired and wireless rogues and threats at Layers 1 through 3. Integration of wIPS into the WLAN infrastructure offers cost and operational efficiencies delivered by using a single infrastructure for both wIPS and WLAN services. The solution includes the following components:

- **Access points:** Cisco access points with Cisco CleanAir® are equipped with silicon-based intelligence to allow for Layer 1 threat detection of attacks that may come from non-802.11 sources, such as video cameras or RF jammers. Access points intelligently process over-the-air traffic to a large library of wireless intrusion attacks and anomalies to determine whether the network is being attacked or impersonation is in progress. This processing occurs on the edge to allow for greater scalability. Access points relay information such as the MAC address of the victim and attacker, received signal strength indication (RSSI),

[1] Cisco Visual Networking Index 2013 Report

and time of attack to the WLAN controllers using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol.

- **Access points with wireless security module:** The Cisco Aironet® Access Point Module for Wireless Security and Spectrum Intelligence aggressively scans all channels without affecting the data-serving radios in the 2.4- and 5-GHz bands.
- **Wireless LAN controller (WLC):** The WLC generates traps to the network management system when security events such as rogue access points are detected or an attack is in progress, as well as mitigates rogue threats as defined by the rogue policy.
- **Cisco Mobility Services Engine (MSE):** Cisco delivers the industry's first location-aware wIPS with the integration of the Cisco MSE. The Cisco MSE receives a list of controllers, access points, and the physical location of access points in the map from Cisco Prime™ Infrastructure, and combines it with real-time information from the WLC, such as MAC address, timestamp, RSSI, and attack IDs. The MSE can correlate security events such as rogues, interferers, and active intrusions by eliminating duplicate security events and computing an x,y location for all valid clients, clients connected to rogue access points, rogue access points, attackers, and non-802.11 interferers.
- **Cisco Prime Infrastructure:** Cisco Prime Infrastructure receives data from the MSE and provides monitoring dashboards, configuration, troubleshooting, reporting, and location on the map for rogue access points, valid clients, and rogue clients. It also offers a consolidated view of rogue alarms and security threats across the network and tools to capture and store forensic data, as well as built-in reports for industry-standard security reports.

Cisco 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.

Solution Benefits

The Cisco wIPS solution offers a superset of capabilities not architecturally possible with standalone, overlay wIPS systems. The infrastructure-integrated architecture of Cisco wIPS allows network administrators to:

- **See the whole picture:** Typical wIPS solutions rely solely on RF air monitoring for detection. Cisco 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 wIPS doesn't just detect threats, vulnerabilities, and performance issues; it makes it possible to take corrective action. Integration into the WLAN infrastructure enables wIPS to go beyond passive monitoring and reach into the infrastructure to fix security threats and performance issues in real time.
- **Take advantage of the entire WLAN footprint:** Cisco 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 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 wIPS analysis engine. wIPS can detect 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 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 and 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 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 Access infrastructure complement the Cisco 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 that follow outline each functional area of the Cisco wIPS solution and the associated benefits.

Rogue Detection, Classification, and Mitigation

Cisco wIPS features rogue detection and mitigation, as shown in Table 1. Rogue access points and clients can create back-door access to your network and can be used for data theft from your wireless clients. wIPS detects, automatically 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- and 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 the breadth and accuracy of rogue, ad hoc, and spoofing detection, thus decreasing time spent on manual threat investigation by staff
Spectrum intelligence	Detects rogue devices and DoS in non-802.11 frequencies, such as Bluetooth, radar, and microwave
Event Classification	
Customizable rogue event automatic classification	Automatically classifies the threat level of rogue events based on user-defined classification rules, thus reducing the need for staff intervention
Rogue switch-port tracing	Establishes whether a detected rogue access point is on the customer network, thus reducing the need for manual staff investigation to assess the threat
Physical location of rogue devices	Plots rogue access points and clients on a floor map, thus helping staff assess the rogue threat and facilitate removal
Mitigation	
Disabling of rogue switch-port	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 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 sitting in the parking lot in front of your office. Attack types include network reconnaissance, authentication and encryption cracking, DoS, 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 DoS 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 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 Cisco Prime Infrastructure, 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 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 Prime Infrastructure management system automatically performs automated, around-the-clock 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, 24x7 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, Cisco Prime Infrastructure delivers greater accuracy and depth of vulnerability analysis, such as analysis of management protocol security and analysis of security services operating on the network
Analysis against industry best practices or custom-defined security policies	Cisco Prime Infrastructure is prepopulated with industry best practices for wireless security vulnerability assessment; Config Audit enables analysis of configurations against the organization's specific security policies. This dual approach enables the greatest flexibility and breadth of vulnerability analysis

Feature	Benefit
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
wIPS alarm consolidation	Consolidate wIPS alarms based on predefined rules. Concise information to the user to determine the real attack or threat
Auto MAC address learning	MSE learns and remembers valid client information and then prevents valid clients from associating with rogue access points
Easy-to-use wizard for wIPS profile	New wireless security wizard workflow reduces setup time to tune the system by defining rogue classification rules
Global forensics	Ability to automatically start and stop packet capture when attacked or on demand for troubleshooting or debugging
Rogue access point zone of impact	Visualize the zone of impact where valid clients have the highest likelihood of connecting to a rogue access point

Performance Monitoring and Automatic Optimization

Cisco 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 actions. Using 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, route around failed devices, and 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
Automatic correction of problems in the RF domain	Remedies issues, such as RF-based DoS, without administrator intervention, thus increasing network uptime with minimal operational overhead
Complete RF management without specialized RF skills	RF management expertise is integrated into the system, thus reducing the burden on operational staff

Management, Monitoring, and Reporting

Cisco wIPS features complete security management, monitoring, and reporting capabilities, as shown in Table 5. wIPS management is fully integrated into Cisco Prime Infrastructure, 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 reducing administrative overhead
Virtualized management domains	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 Cisco Prime Infrastructure, thus reducing staff training and support on disparate platforms
Integration with Cisco Unified Wireless Network features	wIPS provides unified workflows integrating general wireless network configuration, wireless security policy definition, and location service operation

Feature	Benefit
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	Cisco Prime Infrastructure is designed for the highest-scale environments: up to 3000 user-serving or wIPS access points per Cisco Prime Infrastructure instance
Cisco Prime Infrastructure 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 Cisco Prime Infrastructure security dashboard, thus providing a networkwide view of wireless user activity
Cisco Prime Infrastructure 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
Cisco Prime Infrastructure 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
Automatic report 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 PCI compliance, thus streamlining audit-related activities
Event storage and archiving	Security attack events are stored in the Cisco MSE for long-term archiving, thus streamlining historical analysis

Wireless IPS Software

- All Cisco Lightweight Access Point Protocol (LWAPP) access points are supported for Monitor Mode wIPS monitoring.
- All 802.11n LWAPP access points are supported for Enhanced Local Mode (ELM) wIPS monitoring.
- For MSE wIPS scaling information, see the Cisco Mobility Services Engine Data Sheet.

Licensing and Ordering Information

Cisco wIPS is a licensed software feature set on the Cisco Mobility Services Engine and is available for releases 7.0.xxx and later. The ELM feature requires Release 7.4.xxx or later.

For specific licensing information, see the Cisco Mobility Services Ordering and Licensing Guide.

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 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 Cisco Wireless, 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 C78-501388-04 10/13