Data sheet

Cisco public

The bridge to possible

Cisco Advanced Wireless Intrusion Prevention System and Rogue Management

Contents

Solution overview

Wireless is no longer a good-to-have secondary network. With advances and ratifications in Wi-Fi standards, dense environments with many concurrently connecting devices and Internet of Things (IoT) connections result in multiple use cases across industry segments. Today, there are more than 15 billion devices connected through wireless, and this number is expected to grow beyond 20 billion by the end of 2021.[[source: https://www.statista.com/statistics/802706/world-wlan-connected-device/]] Enterprises providing Wi-Fi access to employees and guests, public venues providing hotspots, industrial IoT devices connecting through wireless, and many more situations present a multitude of opportunities but also pose new threats to the network. The total number of global Distributed Denial-of-Service (DDoS) attacks is expected to double from 7.9 million in 2018 to 15.4 million by 2023. [[source: Cisco Annual Internet Report (2018-2023]] 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 ever-changing threats, so IT organizations are constantly challenged to both track and locate wireless threats throughout the organization and demonstrate compliance.

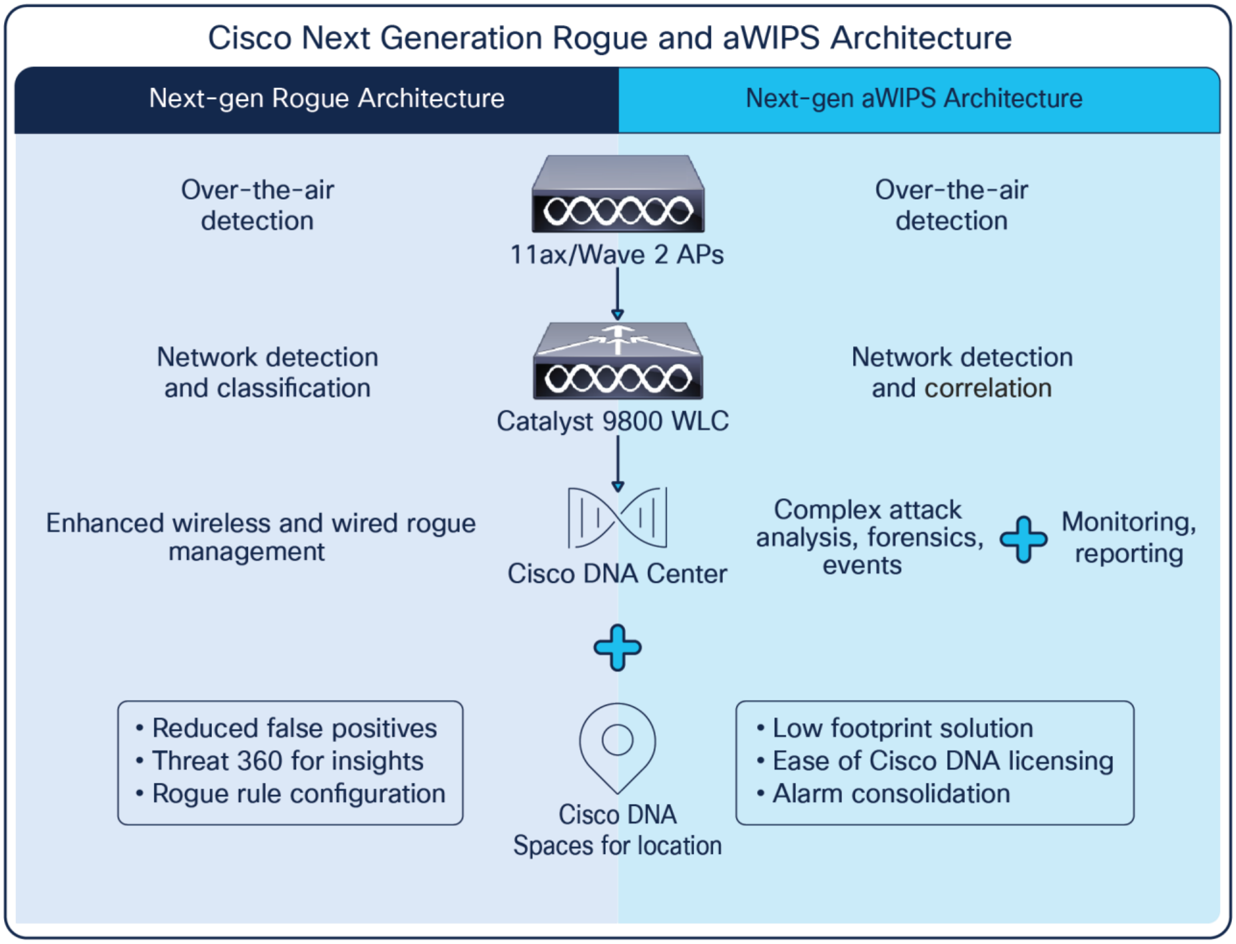
Cisco Next Generation Rogue and aWIPS Architecture
Next-gen Rogue Architecture
Next-gen aWIPS Architecture
Over-the-air detection
11ax/Wave 2 APs
Over-the-air detection
Network detection and classification
Catalyst 9800 WLC
Network detection and correlation
Enhanced wireless and wired rogue management
Cisco DNA Center
Complex attack analysis, forensics, events
Monitoring, reporting
• Reduced false positives
• Threat 360 for insights
• Rogue rule configuration
Cisco DNA Spaces for location
• Low footprint solution
• Ease of Cisco DNA licensing
• Alarm consolidation

Figure 1.
Cisco Advanced WIPS and Rogue Management: System overview

Cisco Advanced Wireless Intrusion Prevention System (aWIPS) and Rogue Management is a complete wireless security solution that uses the Cisco DNA Center and Cisco Catalyst infrastructure to detect, locate, mitigate, and contain wired and wireless rogues and threats at Layers 1 through 3. Integration of aWIPS into the WLAN infrastructure offers cost and operational efficiencies delivered by using a single infrastructure for both aWIPS 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 through a large library of wireless intrusion attacks and anomalies to determine whether the network is being attacked. 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), and time of attack, to the WLAN controllers, using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. The RF ASIC present on Cisco Catalyst 9120 and 9130 access points scans all channels without affecting the data-serving radios in the 2.4- and 5-GHz bands.
- **Cisco Catalyst 9800 Series Wireless Controllers:** The Catalyst 9800 series houses rogue detection and multiple aWIPS signatures logic to determine the type of attack. The Catalyst 9800 Series sends alerts to Cisco DNA Center 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 DNA Center:** Cisco DNA Center is a powerful network controller and management dashboard that lets you take charge of your network, optimize your Cisco investment, and lower your IT spending.

  The Rogue Management application in Cisco DNA Center detects and classifies threats and enables network administrators, network operators, and security operators to monitor network threats. Cisco DNA Center helps in quickly identifying the highest-priority threats and allows you to monitor these threats in the Rogue and aWIPS dashboard within Cisco DNA Assurance. The Threat 360 view on this dashboard provides further details on any specific threat. This includes a map view for quick location, and all affected clients.

Cisco aWIPS and Rogue Management 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 aWIPS and Rogue Management solution offers a superset of capabilities not architecturally possible with standalone, overlay aWIPS and rogue management systems. The infrastructure-integrated architecture of Cisco aWIPS and Rogue Management allows network administrators to:

- **See the whole picture:** Typical aWIPS solutions rely solely on RF air monitoring for detection. Cisco aWIPS and Rogue Management 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 aWIPS and Rogue Management doesn't just detect threats, vulnerabilities, and performance issues; it makes it possible to take corrective action. Integration into the WLAN infrastructure enables aWIPS and Rogue Management to go beyond passive monitoring and reach into the infrastructure to fix security threats and performance issues in real time using containment.

- **Take advantage of the entire WLAN footprint:** Cisco aWIPS and Rogue Management 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 aWIPS and Rogue Management can use access points dedicated to full-time air monitoring or access points serving WLAN users or both. Deployment flexibility is provided by supporting multiple modes like local, FlexConnect central switching, FlexConnect local switching, SDA etc. Cisco DNA Center allows you to group devices based on location, beginning by laying out a hierarchy of areas, buildings, and floors as required to accurately represent the location of your network. A site hierarchy lets you enable unique network settings and IP spaces for different groups of devices. 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 aWIPS analysis, correlation, and classification engine on Cisco DNA Center. aWIPS 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 aWIPS 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, hacker access points such as honeypots and evil twins, network reconnaissance, AP impersonation such as address and identity spoofing, 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 aWIPS 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 Catalyst access infrastructure complement the Cisco aWIPS 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 and spoofing 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 the Wi-Fi Protected Access 3 (WPA3) 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 LSC provisioning or authorization list 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 aWIPS and Rogue Management solution and the associated benefits.

Rogue detection, classification, and mitigation

Cisco aWIPS and Rogue Management 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 to steal data from your wireless clients. The Cisco Rogue Management solution 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 the time staff spend manually investigating threats
CleanAir/Spectrum Intelligence	Detects rogue devices and DoS attacks 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 staff to manually 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 Location accuracy can be improved by integrating with CMX or Cisco Spaces
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 aWIPS 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, and DoS, 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 access point impersonation, honeypot access points, AirDrop sessions, and other methods, providing an early alert that a hacker is looking for avenues of attack
Detection of authentication/cracking and vulnerability exploits	Analyzes traffic behavior and performs pattern matching to detect tools and techniques such as fuzzed beacon, fuzzed probe request, fuzzed probe response malformed association request, malformed authentication, invalid MAC OUI, and other methods, providing an alert to 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, RF jamming, resource starvation using authentication flood, association flood, Extensible Authentication Protocol over LAN (EAPoL)-start flood, PS-Poll flood, probe request flood, reassociation flood, Request-To-Send (RTS) flood, Clear-To-Send (CTS) flood, beacon flood, and other methods, providing an alert of potential or attempted network service disruption. DoS attacks toward clients, such as deauthentication flood, disassociation flood, broadcast deauthentication flood, broadcast disassociation flood, EAPoL logoff flood, authentication failure attack, probe response flood, and block ack flood, can also be detected
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, RADIUS server spoofing, and other methods, providing an alert to 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 to 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 aWIPS 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 DNA Center, giving operators plain-language descriptions of attack types and detection methods as well as tuning guidance, thus making tuning even easier for novice security operators

Security vulnerability monitoring

Cisco aWIPS 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. Cisco DNA Center 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 DNA Center delivers greater accuracy and depth of vulnerability analysis, such as analysis of management protocol security and analysis of security services operating on the network with configuration compliance for out-of-band changes
Analysis for adherence to industry best practices or custom-defined security policies	Cisco DNA Center 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
Broad vulnerability identification through security advisories	Identifies vulnerabilities through Product Security Incident Response Team (PSIRT) scans for vulnerabilities that can result in unauthorized management and network access, data theft, DoS attacks, and protocol attacks, and advises on security services to run on the wireless network
aWIPS alarm consolidation	Consolidates aWIPS alarms based on predefined rules and provides concise information to the user to determine the real attack or threat
Easy-to-use workflows	Wireless aWIPS and Rogue workflows enable users to fine-tune aWIPS signatures and rogue rules by providing the flexibility to select signatures and configure thresholds for signatures and threat levels for rogue rules with conditions
Signature-wise forensics	Ability to automatically start and stop packet capture when attacked for troubleshooting or debugging per signature or threat
Rogue access point zone of impact	Cisco DNA Center Threat 360 view provides a detailed view of each of the alarms, giving the context of the attack, threat level, and location and time of the attack

Performance monitoring and automatic optimization

Cisco aWIPS 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 aWIPS features complete security management, monitoring, and reporting capabilities, as shown in Table 5. aWIPS management is fully integrated into Cisco DNA Center, 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 a high level of accuracy in rogue detection while reducing administrative overhead
Virtualized management domains	aWIPS enables split wireless security management and monitoring from other wireless management roles or geographies
No one-off management platforms	All aWIPS and general wireless management is performed from Cisco DNA Center, thus reducing staff training and support on disparate platforms
Integration with Cisco Unified Wireless Network features	aWIPS 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	Cisco DNA Center is designed for the highest-scale environments: up to 96,000 rogue access points and 13,000 aWIPS access points per 112-core Cisco DNA Center appliance
Cisco DNA Center Rogue and aWIPS Assurance 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

Feature	Benefit
Cisco DNA Center Health 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 DNA Center event management and reporting	
Complete event forensics	Captures all traffic associated with an attack, for ease of investigation
Event escalation to staff	Automatically alerts staff regarding critical events, thus decreasing response time, on the Rogue and aWIPS dashboard in Cisco DNA Center
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
Event storage and archiving	Security attack events are stored in Cisco DNA Center for 14 days, with long-term archiving available out of the box, providing historical analysis

Wireless IPS software

- All Cisco 802.11ac Wave 2 and 802.11ax access points are supported for Monitor Mode aWIPS monitoring and client serving mode with on and off channel scanning. Cisco Catalyst 9120AX and 9130AX Series access points have a built-in RF ASIC-based auxiliary radio that continuously monitors all the channels for rogue and aWIPS detection.
- For information on scaling Cisco DNA Center aWIPS and Rogue Management, see the Cisco DNA Center Rogue Management and aWIPS Application Quick Start Guide.

Licensing and ordering information

Cisco aWIPS is a licensed software feature set included in Cisco DNA Advantage and is available for all the releases. Cisco Rogue management features are available with Cisco DNA Essentials license.

For specific licensing information, see the Cisco DNA Software Subscriptions for Access Wireless Ordering 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 Customer Experience.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

For more information about Cisco aWIPS, visit https://www.cisco.com/go/aWIPS.

For more information about Cisco DNA Center, visit https://www.cisco.com/site/us/en/products/networking/index.html.

For more information about Cisco wireless, visit https://www.cisco.com/go/wireless

Document history

New or Revised Topic	Described In	Date
Cisco DNA Spaces name change	Updated product name to Cisco Spaces	10/21/22

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 **https://www.cisco.com/go/offices**.

Printed in USA C78-501388-08 10/22