Cisco Adaptive Wireless Intrusion Prevention System FAQ

Positioning

Q. How is the Cisco® Wireless Intrusion Prevention System (wIPS) different than network IPS in the Cisco ASA 5500 Series and IPS 4200 Series?

A. Wireless IPS detects wireless-specific attack techniques by scanning the RF airwaves. Wireless IPS does not perform any Layer 3 or higher malware or hacking prevention, whereas network IPS focuses on just that. Network IPS does not detect wireless threats and does not monitor the airwaves.

Q. Are wireless IPS and network IPS substitutes for one another?

A. No. Wireless IPS detects wireless threats only and does so by scanning the RF airwaves. Network IPS does not and cannot detect wireless threats because it does not scan the RF airwaves. They are completely complementary technologies.

Product Components

Q. What are the components needed to build an Adaptive wIPS deployment?

A. The following components are required:

- wIPS monitor mode access point(s): Provides constant channel scanning with attack detection and forensics (packet capture) capabilities.
- Mobility Services Engine (MSE) with wIPS license: The central point of alarm aggregation from all controllers and their respective wIPS monitor mode access points. Alarm information and forensic files are stored on the system for archival purposes.
- Wireless LAN Controller(s) (WLC): Forwards attack information from wIPS monitor mode access points to the MSE and distributes configuration parameters to access points.
- Wireless Control System (WCS): Provides the administrator the means to configure the wIPS service on the MSE, push wIPS configurations to the controller, and set access points into wIPS monitor mode. It is also used for viewing wIPS alarms, forensics, and reporting, and for accessing the attack encyclopedia.

Q. Are there special wIPS models of access points required?

A. No. Adaptive wIPS operates on standard Cisco Lightweight Access Point Protocol (LWAPP) access points.

Q. What Cisco APs are supported?

A. The following Cisco LWAPP access point models: the Cisco Aironet® 1130, 1140, 1240 and 1250 Series.

Q. What model of Mobility Services Engine (MSE) is supported for Adaptive wIPS?

A. The MSE 3310 is supported in the 5.2 release. The MSE 3350 will be supported in an upcoming release.

Features

Q. What is the minimum software release required for the full Adaptive wIPS feature set?

A. Cisco Unified Wireless Network version 5.2 on WLC/AP, WCS and MSE.

Q. What new wIPS functionality comes in Version 5.2?

A. The following new functionality is included in Version 5.2:

- Greater breadth of attack detection: Six times increase detection of attacks and attack tools, as well as ongoing detection updates in future releases
- Anomaly detection for unknown or zero-day attacks
- Attack forensics: Full capture of traffic that spawned the alarm
- Entirely new configuration and tuning GUI in WCS, with full attack and detection descriptions
- Threat knowledgebase with plain-English attack descriptions and response guidance
- Default configuration profiles, by customer vertical, for plug-and-play operation

Q. What other recent features in Cisco Unified Wireless Network 5.0 and 5.1 should I be aware of when considering Adaptive wIPS?

A. See the Adaptive wIPS data sheet or release product bulletins for more information on any of the following features:

- Rogue Event Auto-Classification: Introduced in Cisco Unified Wireless Network Version 5.0, this is a very powerful feature that enables customers to set up classification rules that auto-classify incoming rogue events. This eliminates time-consuming, manual investigation and classification of such events. Accurate event classification is critical to the usability and effectiveness of any wIPS solution.
- Rogue Access Point Switchport Tracing and Disable: Introduced in Version 5.1, this feature traces a rogue access point heard over the air to establish if that rogue is attached to the wired network, and if so, to locate the switchport to which it is attached. Once located, the administrator can also disable that switchport from WCS.
- Automated Security Vulnerability Assessment: Introduced in Version 5.1, this WCS feature scans the wireless infrastructure configurations looking for suboptimal security policies and reports them on the Security Dashboard in a composite score and list of vulnerabilities.
- WCS Security Dashboard: Introduced in Version 5.1, the new, at-a-glance security dashboard provides a single-screen summary of all security events and vulnerabilities presented in a streamlined, quick-scan format.

Q. Do I need an MSE and Adaptive wIPS software license if I just want to do rogue detection?

A. No. Rogue detection capabilities come with the WLAN controllers and WCS. MSE and Adaptive wIPS software licenses are required to detect over-the-air threats such as reconnaissance, encryption cracking, authentication cracking, denial-of-service (DoS) attacks, and potential threats indicated by anomalous traffic patterns. MSE and Adaptive wIPS also provide full-forensics traffic captures, long-term security event archiving, and reporting, wIPS default tuning profiles, and a threat knowledgebase with plain-English attack descriptions and response guidance for ease of operations.

Q. Is it better to use dedicated monitor-mode wIPS access points or shared-user-serving, local-mode access points? What are the differences between the two in terms of rogue detection/mitigation and other wIPS functions?

A. A monitor-mode access point for wIPS spends all of its cycles scanning channels looking for rogues and over-the-air attacks. A monitor-mode access point can simultaneously be used for location (context-aware) services and other monitor-mode services. When wIPS is deployed on a monitor mode access point, the benefits are lower time-to-detection of threats and a broader range of over-the-air threats detected. The Adaptive wIPS Version 5.2 feature set requires monitor mode access points due to the complexity of the attacks that are detected starting in this release.

A local-mode access point splits its cycles between serving WLAN clients and scanning channels for threats. Because of this, it takes a local-mode access point longer to cycle through all the channels, and it spends less time collecting data on any particular channel so that client operations are not disrupted. As a result, detection times are longer (3 to 60 minutes) and a smaller range of over-the-air attacks can be detected than with a monitor-mode access point.

By offering both modes of threat scanning, you customers may choose the deployment model that best fits their security policy, deployment objectives, operational model, and budget.

Q. What is the range of a monitor mode wIPS access point? In what density must they be deployed?

A. A wIPS deployment is based on hearing 802.11 management and control frames which are used by a majority of attacks to cause harm. This is in contrast to a data Access Points deployment which is surveyed to provide higher throughput data rates anywhere from 24Mbps to 54Mbps. There are numerous factors that go into deciding exactly the number of wIPS Access Points that are required for a specific environment. Given that each prospective deployment’s security requirements and environmental conditions are different, there is no hard and fast rule that will address the needs of every deployment but a generalized guideline is that wIPS monitor-mode access point can cover approximately 5-7 times the area of a data access point. This equates to a ratio of 1 wIPS Monitor-Mode AP for every 5 traffic-serving APs at a location as a reasonable starting estimation.

Q. Can the Adaptive wIPS functionality be managed by a separate IT group than the rest of the wireless network?

A. Yes. WCS Partitioning enables subsets of functionality, like wIPS, be managed and monitored by a specific set of personnel. It is common to have a security operations team manage wIPS, while the rest of WLAN operation is managed by a networking operations team.

Q. Does the 802.11n protocol have implications for wIPS and rogue detection?

A. Yes. Given that the 802.11n introduces an entirely new physical layer specification, existing 802.11a/b/g Access Points are unable to decode these new high-throughput data rates as the modulation scheme is fundamentally different. This can leave the wireless network vulnerable to attacks sent out at 802.11n rates with no visibility into these threats as they are essentially invisible to non-802.11n devices.

Although 802.11a/b/g access points can detect most 802.11n rogues because their beacons are sent at legacy rates, only an 802.11n Access Points can detect rogues operating in Greenfield mode. Greenfield mode is a configuration parameter of an 802.11n Access Point that precludes the device from transmitting at non-802.11n rates. While rogues not operating in 802.11n Greenfield mode can be detected, Greenfield rogues and attacks at 802.11n data rates will not be detected by 802.11a/b/g Access Points. Customers are encouraged to utilize the Cisco 1140 and 1250 series Access Points to allow the detection of these 802.11n-based attacks.

Additional Information Resources

Data sheet and other Adaptive wIPS collateral http://www.cisco.com/go/wips.

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 C67-503875-00 11/08