

Enterprise



**A Closer Look at Wireless
Intrusion Detection:
How to Benefit from a Hybrid
Deployment Model**

Josh Wright | Senior Security Researcher

Introduction

As wireless enterprise networks become more pervasive, increasingly sophisticated attacks are developed to exploit these networks. In response, many organizations consider the deployment of wireless intrusion protection and wireless intrusion detection systems (WIPS/WIDS). These systems can offer sophisticated monitoring and reporting capabilities to identify attacks against wireless infrastructure, while stopping multiple classes of attack before they are successful against a network.

Organizations have several options when selecting an architecture for WIDS deployment. These include an overlay approach, which uses dedicated sensors to create an overlay security network; integrated monitoring, which relies on dual-purpose transmission/sensor equipment that also carries customer traffic; and a hybrid approach, which uses elements of both of the other architectures. A closer look at deployment options shows that there are unique benefits and weaknesses associated with each. However, the hybrid model tends to offer the most flexibility and security because it provides focused analysis mechanisms, increased flexibility in deployment and powerful attack detection and response mechanisms. To maximize the benefits of a hybrid approach, however, vendor alternatives must be closely scrutinized to ensure that the vendor provides certain capabilities that are required to fully support a hybrid WIDS deployment. Such capabilities include an integrated identity-based ICSA-certified firewall and extensive wireless intrusion protection capabilities to ensure that the network can respond effectively in the event of an internal or external attack.

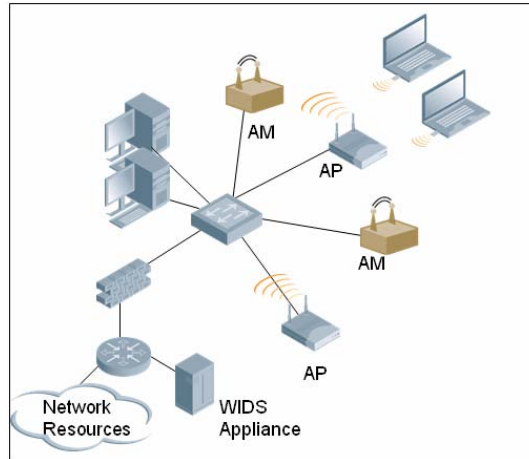
Deployment Approaches

Wireless intrusion detection methodologies have diverged among wireless and security vendors. When selecting a WIDS vendor, it is important to first understand the deployment methodologies supported by each system. The available WIDS deployment models include overlay, integrated, and hybrid.

Overlay Monitoring

In an overlay monitoring deployment, organizations augment their existing WLAN infrastructure with dedicated wireless sensors or “Air Monitors” (AMs). The AMs are connected to the network in a manner similar to access points (APs). They can be deployed in ceilings or on walls and supported by power over Ethernet (PoE) injectors in wiring closets. While APs are responsible for providing client connectivity, AMs are primarily passive devices that monitor the air for signs of attack or other undesired wireless activity.

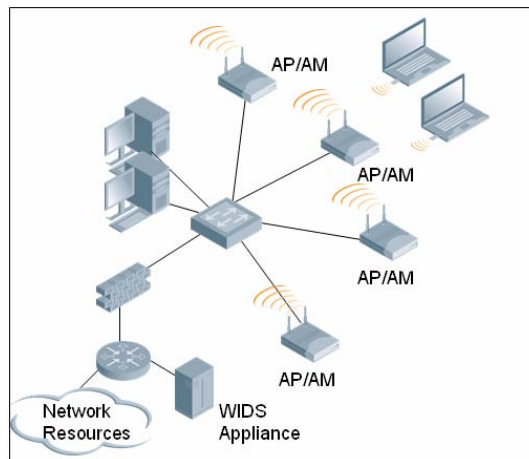
In an overlay WIDS system, the WIDS vendor provides a controller in the form of a server or appliance that collects and assesses information from the AMs that is monitored by an administrator. These devices do not otherwise participate with the rest of the wireless network, and are limited to assessing traffic at the physical layer (layer 1) and the data-link layer (layer 2).



Overlay WIDS Example

Integrated Monitoring

In an integrated monitoring deployment, organizations leverage existing access point hardware as dual-purpose AP/AM devices. APs are responsible for providing client connectivity in an infrastructure role, and for analyzing wireless traffic to identify attacks and other undesired activity at the same time. This is often a less-costly approach compared to overlay monitoring, since organizations use existing hardware for both monitoring and infrastructure access without the need for additional sensors or an overlay management controller.

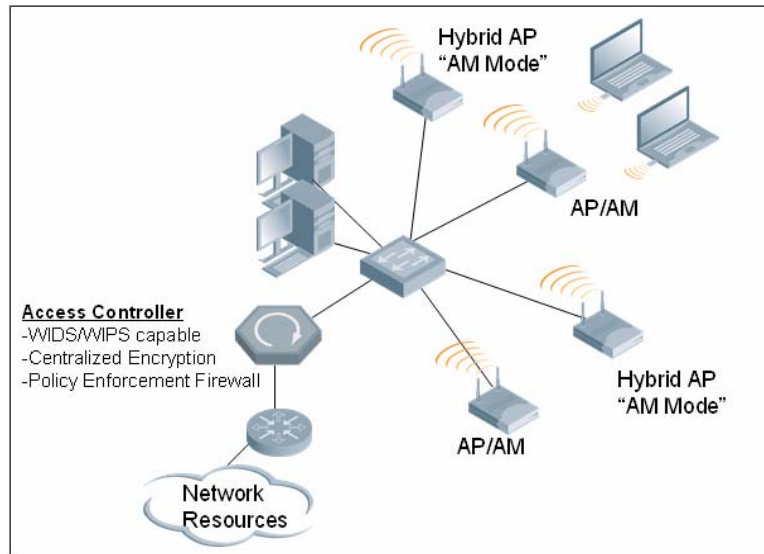


Integrated WIDS Example

Hybrid Monitoring

A hybrid monitoring approach leverages the strengths of both the overlay and integrated monitoring models. A hybrid approach uses both dual-purpose APs and dedicated AMs for intrusion detection and protection. Organizations can use an existing deployment of APs and augment that protection with dedicated AMs, or deploy a dedicated monitoring infrastructure consisting solely of AM devices. In either case, analysis is

performed by a centralized controller similar to what is used with an overlay model, rather than the approach used in an integrated WIDS deployment, where processing is handled by distributed access points.



Hybrid WIDS Example

Strengths of Hybrid Monitoring

The hybrid WIDS deployment model offers several advantages over the integrated or overlay models including increased flexibility in deployment, focused analysis mechanisms, more comprehensive attack detection and powerful response mechanisms.

Deployment Flexibility

By leveraging the benefits of an integrated monitoring model, organizations that have dual-purpose APs deployed for wireless access can take advantage of their existing hardware investment while gaining the security advantages of centralized WIDS monitoring and reporting. In a centralized encryption and processing model, all wireless traffic is handled at an Access Controller (AC). Unlike an integrated WIDS deployment that uses the limited processing capabilities of distributed access points for analysis, a centralized AC can provide the additional resources needed for intensive WIDS analysis.

Alternatively, organizations looking to augment their existing wireless infrastructure with a WIDS monitoring component can deploy a hybrid WIDS network using AM devices. Although the cost structure is similar to that of a standard overlay network, the advantage is that, unlike with a standard overlay network, some AMs are not limited to performing only WIDS monitoring, and can be dynamically changed from an AM to an infrastructure AP as needed. This allows organizations to deploy AMs today to meet their monitoring needs, with the option of adding APs in the future for wireless infrastructure networking.

Focused Analysis

A major benefit of the hybrid model is that it allows organizations to apply WIDS techniques not only to traffic from their own infrastructure, but also to any wireless traffic within range of deployed AMs. This approach provides stronger analytical capabilities than either the overlay or integrated WIDS approach.

In an integrated WIDS deployment, infrastructure APs are responsible for assessing traffic to identify attacks. While this is the best approach for monitoring the authorized infrastructure network, it is limited in its ability to assess threats on wireless channels and frequencies other than those for which the wireless network is currently configured.

The most significant limitation in the integrated WIDS deployment model is the inability to freely scan other frequencies for attack activity, including rogue AP devices. When the access point is responsible for providing client connectivity and responding to traffic sent by associated wireless clients, it is not free to scan other frequencies for attack activity. (This scanning capability is also known as channel hopping). While some integrated deployment vendors have augmented their APs to scan other channels, there is a significant performance detriment: stations cannot transmit or receive traffic while the AP is scanning other channels.

In an overlay WIDS network, dedicated AMs are responsible for analyzing wireless traffic, and are usually deployed with a channel hopping algorithm so they can analyze traffic on all available frequencies. This approach is effective at identifying noisy attacks, such as a rogue AP that is transmitting frequent beacon frames, or a flood attack, as is common with IEEE 802.11 denial of service (DoS) vulnerabilities. However, because AMs are configured for channel hopping, they are not the most appropriate monitoring mechanism for analyzing a wireless network that is operating on a single channel for a given area. While the AM is scanning other frequencies, it is likely that the sensor will miss attacks that target the production network.

Further, AMs are often deployed with no knowledge of the operating characteristics of the production network. Even if the AM is configured to monitor a single channel that is used by the production network for a given area, the channel selection and configuration is applied independently of the AP. If the administrator changes the channel configuration of the AP or if the AP changes the channel configuration dynamically to avoid interference with other RF sources, the AM must be adjusted to reflect this change as well. This can represent a significant operating burden for the WIDS administrator in the best case, or the inability to monitor the production network altogether in the worst case.

Fortunately, a hybrid approach from the right vendor can address the limitations of both overlay and integrated monitoring systems. By augmenting the integrated wireless infrastructure with AM devices, the hybrid model has the freedom to perform analysis while channel hopping to identify rogue AP devices and attacks on channels not currently used by infrastructure components. To mitigate the intermittent monitoring

capabilities of an AM that is channel hopping, all traffic should pass through a centralized access controller and should be subject to WIDS analysis, thus providing a constant monitoring mechanism.

Location Services

The ability to locate the source of an attack or potentially problematic areas is another valuable feature for WIDS systems. Nearly all WIDS vendors offer some sort of location-based identification service, with varying degrees of success.

Location services are commonly implemented by examining the receive signal strength of frames based on the source MAC address and triangulating the information with data from other sensors to estimate the location of the transmitter. While this mechanism works well for unsophisticated attacks such as rogue AP identification, it does not provide reliable location reporting when an attacker uses MAC spoofing attack techniques.

In a MAC spoofing attack, the attacker will transmit malformed frames into the network by impersonating a valid station or access point. This is problematic for location reporting algorithms, since the algorithm is unable to differentiate legitimate and illegitimate receive signal strength indication (RSSI) for the same source MAC address.

Vendors that implement a WIDS implementation where the data path is integrated and all encrypted traffic is terminated at a centralized mobility controller will have unique visibility into the network to easily identify and discard spoofed frames from an attacker. This approach enables the system to more reliably identify the location of an attacker, rather than the legitimate client system.

Comprehensive Attack Detection

An additional limitation of an overlay WIDS network is the inability to assess the contents of encrypted wireless traffic. An overlay WIDS approach is heavily focused on the assessment of physical layer (layer 1) and data-link layer (layer 2) traffic. When organizations deploy strong encryption mechanisms (operating at higher layers) to protect the wireless network such as WPA/WPA2 or IPSec/VPN, the overlay vendor's AM becomes unable to assess the contents of encrypted wireless traffic.

This weakness in WIDS systems is readily recognized by attackers, who may choose to target vulnerable wireless stations with upper-layer protocol weaknesses such as those found in the client operating system. Information security professionals agree that the majority of attacks initiate within the organization, making wireless networks a prime candidate for an insider to exploit local workstations while evading WIDS monitoring capabilities.

A hybrid WIDS approach solves this problem with centralized encryption in the access controller. With centralized encryption, the AC has knowledge of all dynamic encryption keys used for WPA/WPA2 and

IPSec/VPN networks, and is able to decrypt packets in real-time to assess all layers of wireless traffic. This allows organizations to integrate traditional intrusion detection systems such as Snort with the AC for a comprehensive assessment of attacks on the wireless network. This is an advantage over the traditional overlay model, which does not have knowledge of dynamic encryption keys to decrypt traffic. The disadvantage of the integrated approach, on the other hand, is that distributed AP hardware does not offer a centralized location for an IDS sensor to inspect traffic.

Powerful Attack Response

To mitigate attacks on the wireless network, WIDS vendors have augmented the analysis components of their products with reactive components, often known as Wireless Intrusion Prevention Services (WIPS). When the analysis mechanism recognizes an attack, such as an attempt at accelerated WEP key cracking, the wireless device reacts to the event by reporting it to the administrator and by taking steps to prevent the attack from succeeding.

In an overlay WIDS implementation, the AMs are not involved in the management and operation of the wireless infrastructure and must seek an alternate mechanism for stopping an attacker from communicating on the network. The common mechanism implemented among overlay vendors is to take the previously passive AM device and turn it into an active device that mounts a counter-attack, often deployed as a DoS attack against the wireless station.

While this technique is suitable for defending against rogue AP threats, it has the disadvantage of taking an otherwise passive device (the AM) and turning into an active device. This allows the attacker to use traffic fingerprinting techniques to determine sensitive information about the network, including the characteristics of any WIDS system present. This information gives the attacker an additional opportunity to exploit the network, and to possibly evade detection by the WIDS system altogether.

In an integrated WIDS implementation using distributed APs for wireless transport and monitoring, an AP that detects an attack can simply terminate network connectivity for the offending client station, updating a local blacklist of stations that should no longer be allowed to use the network. This is an effective mechanism for stopping access at a single AP, but it does not offer protection when the attacker roams to another AP. In order to be effective, the client must be blacklisted at every location in the network, independent of the AP with which the client attempts to associate. This is best accomplished with a hybrid solution that uses a centralized access controller that integrates an identity-based ICASA-certified firewall. Integration of a firewall allows for automatic synchronization of the entire WLAN to take the same action against a blacklisted target.

Advantages of an Aruba Hybrid Solution

Aruba Networks provides a comprehensive hybrid deployment approach, giving customers the greatest level of flexibility. In addition, an Aruba solution provides advanced encryption, authentication and access control

mechanisms that are unique to its centralized architecture. Extensive wireless intrusion protection capabilities along with an integrated policy enforcement firewall make an Aruba solution unrivaled in its ability to contain intrusion threats

Blacklisting

Unlike the integrated deployment model using distributed processing on individual access points, the Aruba hybrid approach can centrally blacklist an offending workstation to prevent all access to the network. With this approach, the wireless client is lead to believe that the infrastructure network has effectively disappeared from its view. This functionality is enabled by a stateful ICASA-certified firewall integrated in the Aruba Mobility Controller. The firewall provides blacklist rules that will apply throughout the entire network, regardless of where the offending user or device attempts to roam or re-authenticate.

Dynamic Role Changes

Another benefit of the Aruba hybrid approach for WIPS service is the ability to dynamically change the access privileges of a wireless client using the integrated role-based firewall. When the Aruba Mobility Controller recognizes a configured event from a wireless station (such as a traffic policy violation), the network access privileges of the client can be dynamically changed, thereby restricting the client's access to network resources. In contrast to segmenting users into common broadcast domains using VLANs, firewall roles are a much more secure, scalable and flexible way to segregate user groups and can be easily adjusted as required.

Support for Devices with Weak Encryption

A common requirement for enterprise wireless networks is to improve security for devices with legacy encryption mechanisms such as WEP. In many cases, organizations recognize the weaknesses in the WEP protocol but must support WEP networks for legacy devices such as handheld scanners or VoIP phones. Such support is difficult to achieve without exposing the organization to attacks that exploit weaknesses in the WEP protocol. The Aruba solution allows an administrator to assign restrictive firewall policies to devices that connect with legacy encryption mechanisms, ensuring that they cannot compromise network security. For example, a VoIP handset can be allowed to communicate using SIP only to the VoIP gateway.

Legacy Protocol Support

By leveraging dynamic role assignments in the Aruba hybrid approach, organizations can limit their exposure with legacy wireless protocols. An administrator can establish network privilege assignments for legacy devices that will only grant access to the servers, networks and ports that are required. Under normal traffic conditions, this satisfies the needs of handheld scanners or VoIP phones so they can operate as needed to support the organization.

Network Access Policy Enforcement

In the event that an attacker attempts to exploit the network and gain access to network resources that are not explicitly permitted, the Aruba solution dynamically revokes privileges for the station. The level of privilege that is revoked is identified by the administrator and can range from blacklisting the client to

revoking access to specific services. The system can even notify the station that it has violated a network policy, including instructions for how to restore its network privileges.

Conclusion

Organizations have many options for WIDS/ WIPS service offerings, each presenting various strengths and weaknesses. Overall, a hybrid approach offers distinct advantages over alternative models by offering deployment flexibility, focused analysis and improved attack detection and response capabilities. When selecting a vendor to add intrusion detection and protection to the wireless infrastructure, carefully consider the architecture of the vendor's offering to truly understand the strengths and limitations of the product.

About Aruba Networks, Inc.

Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable follow-me applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.

© 2007 Aruba Networks, Inc. All rights reserved. Specifications are subject to change without notice.

Aruba Networks, BlueScanner and RFprotect are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders.

WP_WID_US_071217



1322 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | info@arubanetworks.com
<http://www.arubanetworks.com>