Securing Your Airspace with WatchGuard's Wireless Intrusion Prevention (WIPS)

Introduction

The proliferation of Wi-Fi across the globe has created an attractive opportunity for cyber attackers to snoop, steal, and infect unsuspecting users' data and systems. As of the publication of this document, there are over 300,000 videos on YouTube explaining how to hack Wi-Fi users with simple-to-use but highly powerful tools easily found online. Offering Wi-Fi within your business – whether for employees or for customers and guests – shouldn't invite such malevolent activity. In this feature brief, we will describe how WatchGuard's Wireless Intrusion Prevention System (WIPS) solves this problem. WIPS is available with WatchGuard cloud-ready access points when managed by the WatchGuard Wi-Fi Cloud.

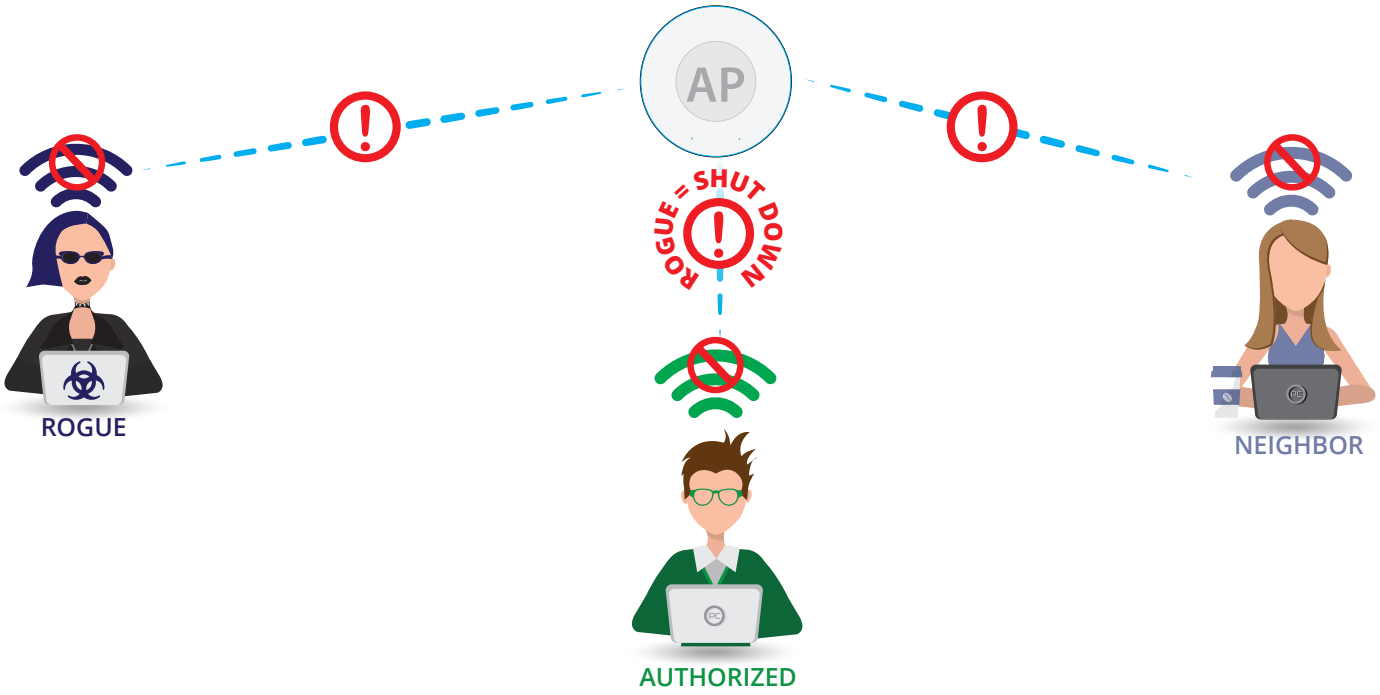
Current solutions fall dramatically short

Competing wireless intrusion prevention systems mostly focus on detection – rather than prevention – for concern of interfering with legitimate neighboring Wi-Fi networks. This is due to the large number of false positives detected by competing solutions, which can lead administrators to ignore the alerts or turn notifications off altogether, leaving their organizations unprotected. Competing WIPS technologies available today require a high level of administration and often provide less than trustworthy rogue AP detection. Organizations that depend on these inadequate systems often have an erroneous sense of security as their networks are in fact vulnerable to breaches via rogue APs.

Own your airspace

With WatchGuard's WIPS, enterprise-grade security can be delivered to a Wi-Fi network with minimal administrative overhead for businesses requiring adherence to compliance standards such as PCI, HIPAA, and Sarbanes Oxley. WatchGuard WIPS leverages patented Marker Packet technology to provide the most rock-solid, reliable, and lowest false positive WIPS in the industry, giving anyone the power to own their Wi-Fi airspace.

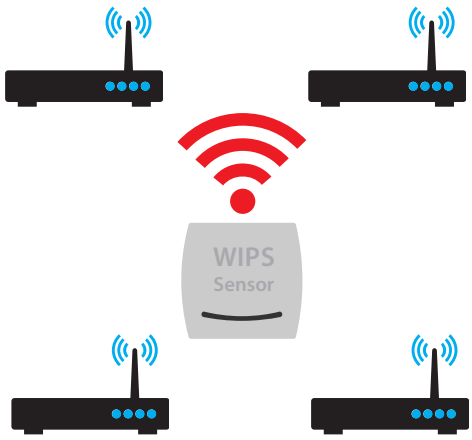
How Do I Enable and Deploy WatchGuard's WIPS?



WatchGuard WIPS is supported on all cloud-ready access points when managed by the WatchGuard Wi-Fi Cloud with active WatchGuard Wi-Fi Cloud licenses. The deployment of WIPS can be achieved in two ways:

1. Recommended: dedicated WIPS sensors

This deployment option involves configuring cloud-ready APs as dedicated WIPS sensors. As a dedicated WIPS sensor, the AP will not allow any wireless clients to connect to it and instead is installed side-by-side with other APs that are configured to handle client traffic. A general rule of thumb for WIPS sensor-to-AP coverage is to install one WIPS sensor for every four APs. This is the recommended deployment model suggested by WatchGuard, providing the securest wireless environment by having dedicated WIPS sensor radios constantly defending the airspace and preventing attackers from taking advantage of time slice windows created by a shared AP/WIPS mode radio.



2. Shared WIPS/AP radios

All cloud-ready APs can be configured to share a portion of their radios' time (as a percentage) between handling wireless client traffic and scanning for WIPS. In this mode, a single AP acts as both an access point and WIPS sensor; however the wireless-side packet injection functionality is not available.

Dedicated Scanning	Background Scanning
Radio dedicated to scanning – dual-band round robin scanning (each channel scanned for 100 ms every 5 second)	Radio operating as AP with dual-band scanning in the background (off-traffic channel scanned for 100 ms every 2 minute)
Fast threat detection on all channels	Off-traffic channel threat detection can take time (still best in industry for rogue APs as Marker Packets™ injection is timed with channel visits)
Can do both over-the-air and over-the-wire prevention. This provides blocking for all threat types.	Only over-the-wire prevention (blocks rogue APs with wireside tarpitting)
Main application: High security/compliance-sensitive environments (financial, government, healthcare, technology, schools, etc.)	Main application: Retail PCI compliance

How WatchGuard's WIPS Works

Wired-side marker packet injection

WIPS injects Marker Packets into the wired network from the wired side of a WIPS/AP. These packets are relayed to the wireless side by APs that are connected to the monitored wired network, which are then detected over the air by the wireless side of the WIPS/AP. The AP may be placed in a subnet or on a trunk port of a managed switch for multiple subnets.

Advantages of this technique are:

- It does not require intrusive interaction with the switches in the network
- It does not require any initial or ongoing configuration to be operational
- This technique quickly detects the APs' connectivity irrespective of the size of the network, since it operates on each local subnet simultaneously
- The volume of traffic generated due to packet injection is negligible (less than 0.1% of the LAN port capacity)
- This technique is free from false alarms in that it never marks rogue APs as external APs; nor does it mark external APs as rogues

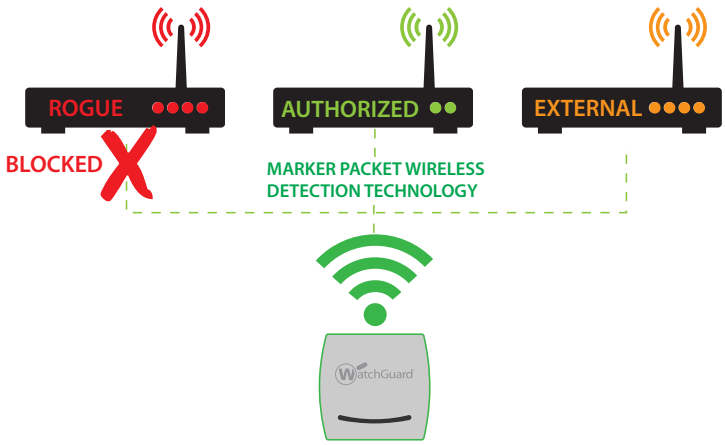
Wireless-side marker packet injection

Once the WIPS/AP sees a client associated to an AP, it sends packets with a unique identifier (Marker Packets) from the wireless side of the potential rogue AP directed towards the IP addresses of a known wire-side host. These packets are piggybacked on the client's link with the potential rogue AP. If any of these packets are received at the target host, the AP is confirmed to be connected to the monitored wired network.

Unique differentiator: auto-AP classification

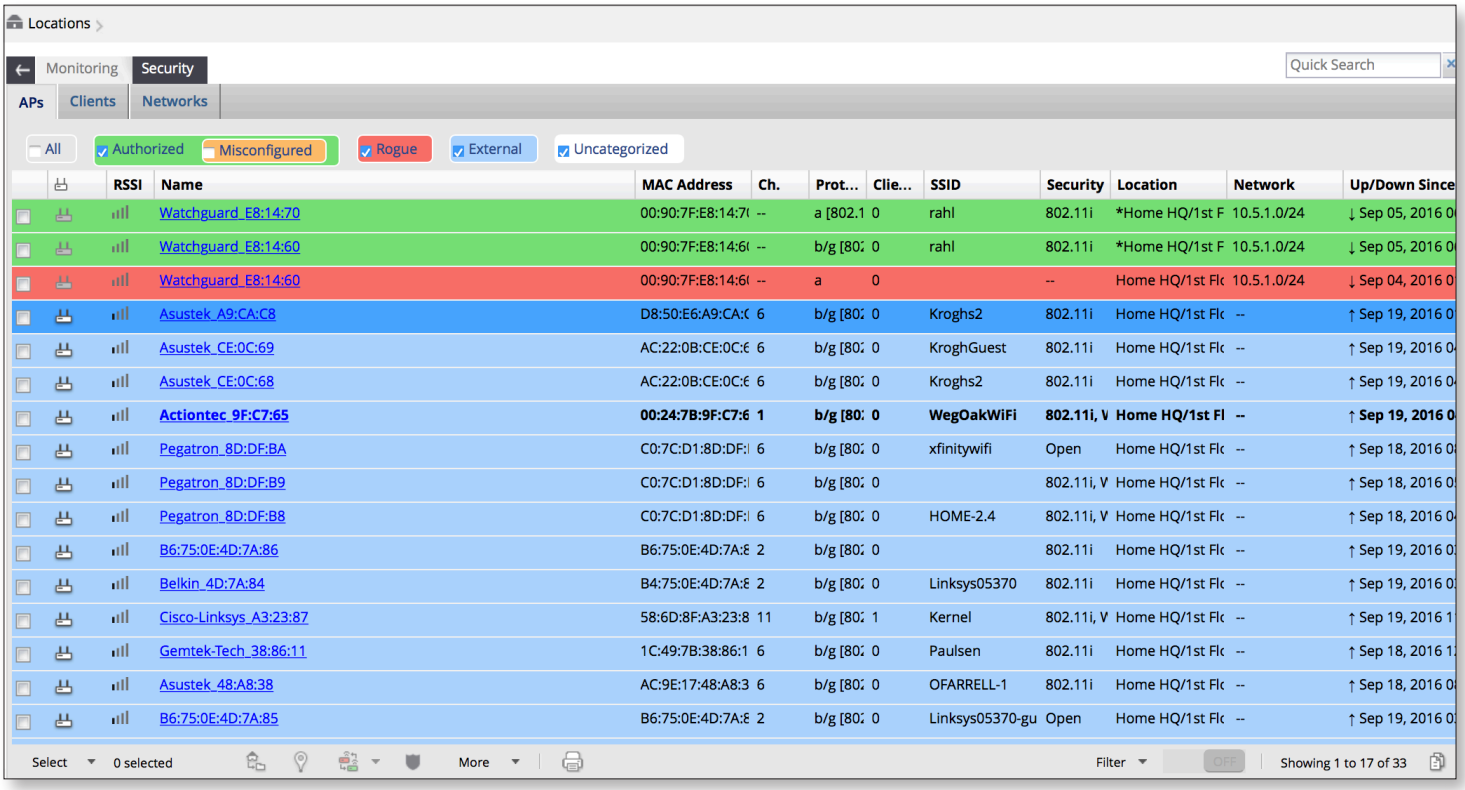
The most natural and elegant way to classify APs is via network connectivity detection. This type of auto-classification does not require unreliable or unmanageable classification signatures based on SSID, vendor, power level, encryption setting or channel; all it needs is reliable network connectivity and access to the desired VLANs.

Accurate, dependable AP auto-classification is a key to an effective Wireless Intrusion Prevention System. WatchGuard's WIPS is the only technology that provides built-in AP network connectivity-based auto-classification. This is made possible by our use of unique Marker Packet technology, which accurately detects network connectivity of all types of APs. The Marker Packet technology is a true differentiator in the WIPS solution space.



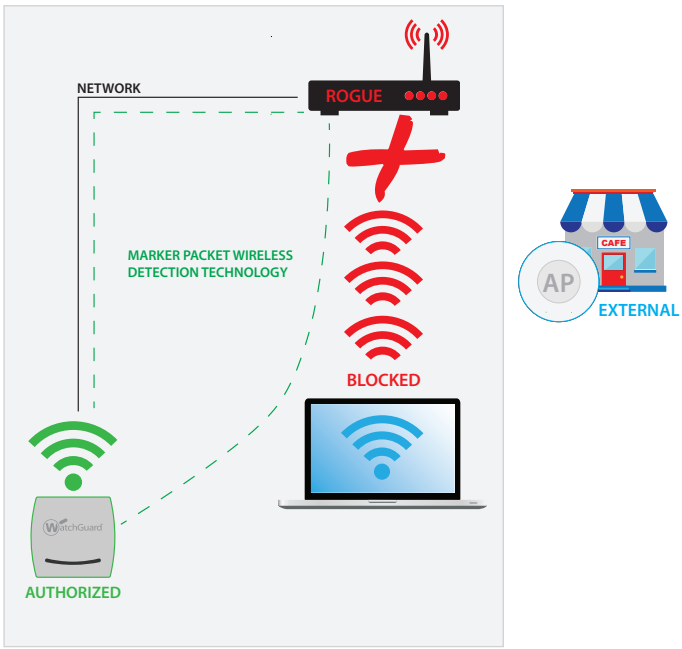
AP auto-classification places visible APs into three categories:

- **Authorized** – Managed APs in the wired network, which the administrator knows about
- **External** – Unmanaged APs in the wireless neighborhood, which are not connected to the monitored wired network
- **Rogue** – Unauthorized APs installed in the wired network without administrator knowledge



Advantages of WatchGuard WIPS:

- Real **prevention**, not just **detection**
- Marker Packet technology
- Accurately classifies devices on the wire with near zero false positives
- Detects, classifies and prevents NAT'd, encrypted, and soft APs
- Detects and blocks unauthorized client behavior
- Auto prevention without harming neighboring devices or networks
- Multiple threat prevention across multiple channels from a single sensor
- Blocks multiple types of 802.11 DoS attacks
- Wireless policies enforced per VLAN, SSID, and location
- Multi-VLAN support (up to 100 VLANs from a single sensor)
- Does not rely on CAM table look-ups or SNMP
- Mobile device watch list
- Off-line sensor mode (always-on security)
- Remote packet capture (R-PCAP) from any sensor
- Most accurate location-tracking from single sensor
- Ability to manage thousands of sensors from a single console
- Various automated security and compliance reports
- Ease of use and deployment / lowest TCO
- Exceeds DoD 8100.2 WIDS requirements
- Provides constant "no Wi-Fi" policy enforcement on wired VLANs in the network

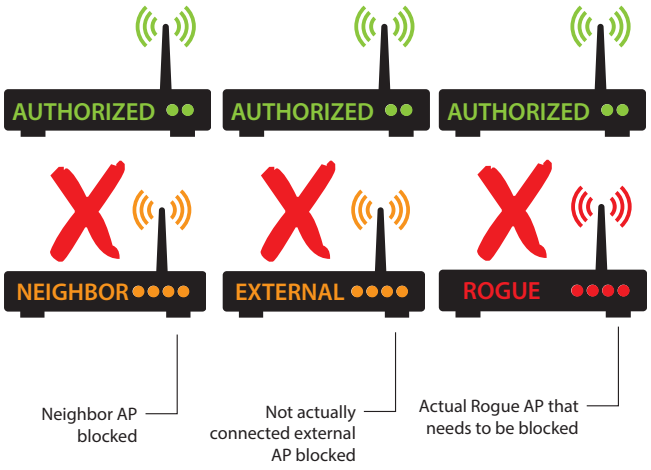


5 Pitfalls of Competing WIPS Solutions

All WIPS are NOT created equal and to help illustrate that point, consider these five pitfalls found in most competing WIPS solutions on the market:

1. Competing rogue AP detection

Rogue APs can be defined as any unauthorized AP that is connected to an authorized network. Rogue APs are a serious threat to networks as they allow unauthorized wireless access to the private network. Rogue APs can appear on the network caused involuntarily by employees or due to malicious attempts of insiders. Many competing WIPS solutions utilize a flawed method to detect rogue APs in the LAN by declaring every AP seen in the air that does not belong to the list of authorized APs as rogue.



Such an approach has the following disadvantages:

- **False alarms**: a security alert would be raised even if the non-authorized AP is seen in the air but not actually connected to the monitored wired network and as such does not pose any security threat.
- **Manual intervention**: the system administrator has to manually examine the non-authorized APs visible in the air to decide which of them are actual rogue APs and which of them are external APs (i.e., neighbor APs).
- **No automatic instantaneous prevention**: since it is highly undesirable to block neighbors' APs accidentally or indiscriminately, instantaneous and automatic blocking of rogue APs is not possible with such an approach.

2. Competing signature-based WIPS

Many competing WIPS attempt to classify APs based on user-configured classification signatures. A myriad of AP properties such as SSID, vendor, power level, encryption settings and channels are used to define classification signatures. Network connectivity of the AP to the network may or may not even be a factor in classification rules. This approach has several disadvantages:

- **Maintaining signatures:** significant configuration overhead is involved in defining classification signatures. The signatures need to be regularly updated, e.g., what happens when a known friendly neighborhood WLAN configuration is changed to use a different SSID?
- **Ongoing manual intervention**: wireless configurations of newly detected APs may not exactly match the defined signatures, in which case, manual intervention is required to classify the newly detected APs.
- **Missed threats:** this approach often misses genuine threats. For example, a classification signature, such as: if "SSID = freewifi AND signal strength = Low"; then classify as known neighbor AP, will be evaded by a rogue AP with low transmit power whose SSID is configured to be "freewifi."

3. Competing MAC table lookup

This technique compares MAC addresses of wireless devices visible in the air with MAC addresses registered at the ports of managed switches in the wired network. If a common MAC address is found between the wireless and the wired sides, it is determined that the device with that MAC address is connected to the monitored wired network.

In the case of bridging APs, detection must wait until a client connects to the AP. After the client connects, its MAC address gets registered in the switch port where the AP is connected. Collection of MAC addresses registered at the ports of managed switches in the network is performed by polling the CAM tables of each switch over SNMP.

This suffers from several disadvantages:

- This technique is intrusive on switching infrastructure. It requires maintenance of switch credentials in the WIPS so that it can poll MAC tables of the switches. It also suffers from interoperability problems with switches from different vendors.
- MAC table polling of all managed switches in the network is a resource-intensive and time-consuming task, especially in large networks with hundreds of switches. Thus, in large networks, network connectivity detection with this approach can only happen infrequently.
- There is a "luck" factor involved in detection. A client's MAC entry disappears from the MAC table after the client becomes inactive, so when MAC table polling occurs (this is typically scheduled at periodic intervals) the technique is only successful while the client is actually connected to the rogue AP.

4. Competing passive MAC correlation

This method attempts to overcome MAC table lookup disadvantages. In this technique, the WIPS AP passively listens on its wire-side interface for MAC addresses that are active on the subnet. MAC addresses discovered by this technique are used for wired/wireless MAC address correlation. However, even this approach suffers from an issue wherein APs not connected to the monitored network, such as neighbor APs, can appear connected to the monitored wired network. This occurs when clients flip between these APs.

5. Competing wireless-side tracing

In this technique, after a WIPS AP detects an AP in the air, it will try to actively connect to the AP on the wireless side. The WIPS AP then either pings something on the wired network through the potential rogue AP or sends a packet to a known host on the wire-side of the network, to try to detect if the AP is connected to the enterprise wired network. This approach of actively connecting to the AP has limitations, in that it takes a fair amount of time for the AP to connect to the AP by completing a L2 and L3 connection (for example, up to 5 seconds). During this time, the WIPS AP needs to be locked on the AP's channel and cannot perform its scanning function. Thus, in the presence of large number of potential rogue APs visible to the WIPS AP, this technique can only be executed infrequently, thereby causing large latency in the detection of AP connectivity. Moreover, this technique fails to detect rogue APs which may have special settings, such as an authorized client MAC address list on the wireless interface, which can prevent the WIPS AP from actively associating to the potential rogue AP.

Combine Best-in Class WIPS with UTM

The driving principle behind every innovative product from WatchGuard is to deliver enterprise-grade security that fits into small and midsize environments. With the WatchGuard Wi-Fi Cloud, IT pros can deliver the high performance wireless connectivity their users demand – without compromising on security – by combining the world's leading WIPS technology with best-in-class UTM services.

Visit www.watchguard.com/wifi to learn more about WatchGuard's family of Secure Wi-Fi solutions.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **watchguard.com**.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com