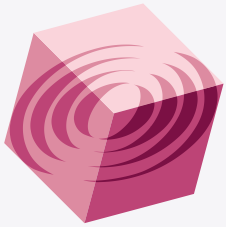


AirTight NETWORKS

The New Threat to Enterprise Security – Wi-Fi

339 N. Bernardo Avenue, Suite 200 • Mountain View, CA 94043
www.airtightnetworks.net

The New Threat to Enterprise Security – Wi-Fi

AirTight NETWORKS

The New Security Challenge

With the rapid adoption of Wi-Fi networks by enterprise IT departments everywhere, network security now involves an entirely new dimension of vulnerability to malicious hackers and casual intruders. Applications and data have literally taken to the airwaves, thanks to the compelling productivity and efficiencies gained by mobility tools such as notebook PCs, handhelds and Blackberries. Companies integrating Wi-Fi are also reaping lower IT infrastructure overhead from fewer cables, faster deployment/redeployment and reduced failure rates associated with hard-wired networks.

The downside is that making corporate data accessible through Wi-Fi networks means intruders and other unwanted visitors can easily access such networks if proper precautions and tools aren't used to protect them. Conventional network firewalls, VPNs and 802.11 security standards do not prevent everyday Wi-Fi threats such as rogue access points, unauthorized client connections and ad hoc networks or more malicious hacking threats like honey pot APs, MAC spoofing and denial of service (DoS) attacks.

Until recently no solutions were available that adequately protected both wireless and wire-line networks by providing automatic and reliable prevention against "rogue" intruders and neighboring unauthorized Wi-Fi clients. A new class of solution, the Wireless Intrusion Prevention System (WIPS) Firewall, is now available to complement wired security solutions such as VPNs and firewalls, providing complete protection of an enterprise's air space and thus their trusted wire-line network. This solution must become widespread if Wi-Fi is to continue its expansion into enterprise as a primary network for mission critical applications.

The Misconception: "No Wi-Fi" Policy Keeps My Network Safe

One of the biggest misconceptions is that an enterprise with a "no Wi-Fi" policy is immune to wireless threats. This perception is due to the fact that many IT administrators presume that without Wi-Fi infrastructure, they are safe from wireless threats. Unfortunately, even with a "no Wi-Fi" policy, Wi-Fi is very likely entering your enterprise through embedded clients in laptops or rogue access points. Over 55% of laptops shipped in 2003 include embedded Wi-Fi , thus an enterprise is likely to have wireless within its premises. Access points are now commonly available in retail stores and on the Internet for less than $30. A recent Gartner survey showed that over 20% of enterprise CIOs had found unsecured access points on their network. Once behind the firewall, these devices are presumed 'safe' and if unsecured provide anyone in range with access to your network, potentially exposing confidential data about your business, customers, products and services.

And, the benefits of using Wi-Fi for productivity gains are too great to sacrifice due to security concerns. Wi-Fi can be deployed securely, and the enterprise can proactively scan and prevent wireless threats without significant burden on the IT department.

Wireless Threat Categories

Wireless threats fall into two general categories, common and malicious, with several types of threats within each group.

Common Wireless Threats

Rogue Access Points

The most common, as well as most dangerous, wireless threat is the rogue access point. The rogue access point is typically a low cost, SOHO-class access point brought in by an employee who desires wireless access. The default access point settings typically have no security enabled, and thus when plugged into the corporate network create an entryway for anyone with a Wi-Fi client within range.

Mis-configured Access Points

For those enterprises with a wireless LAN infrastructure, one potential threat can arise from their own equipment. An access point which becomes mis-configured can potentially open up a door to the corporate network. In particular, if the access point is reset to network defaults or the security settings are turned off. If the access point is not centrally managed, then the likelihood of it going unnoticed is high. Employees will still be able to connect so no problem will be reported.

Client Mis-associations

Embedded Wi-Fi clients in laptops are now relatively common. Even for those enterprises with a "no Wi-Fi" policy, a Windows XP laptop with a wireless client will automatically try to connect to an SSID that it has successfully connected to before. This scenario is very common for two reasons.

If the employee has connected to a Linksys, Netgear or other home or hot spot access point using the default SSID, it will automatically connect to another AP with the same SSID without the user being aware of the connection.

Secondly, neighboring Wi-Fi networks can spill into the enterprise and curious users connect to these open, insecure, and distrusted networks while still connected on the wired side of the trusted network. Users may also connect to these networks if their internal network firewall does not permit POP email accounts, does not permit access to certain web sites, or they do not want their outbound traffic monitored.

Ad Hoc Connections

Wireless clients can also create peer-to-peer connections. A peer-to-peer connection can be exploited by a malicious hacker who may try to then inflict a variety of attacks on the client such as port scanning to explore and exploit client vulnerabilities.

Malicious Wireless Threats

Evil Twin/Honey pot Access Points

Malicious hackers are known to set up Honey pot APs with default SSIDs (e.g. Linksys, Netgear, default, any etc), hotspot SSIDs, and even corporate SSIDs outside of buildings and watch a large number of clients automatically connect to the AP. These APs can then inflict a variety of attacks on the client or attempt password stealing by presenting a login page to the client over the mis-associated wireless connection.

Rogue Clients

Rogue clients are those that are unauthorized to attach to an authorized corporate wireless network. This may occur through an authorized access point that has been mis-configured with encryption turned off, or through an access point that has had its encryption/authentication compromised and uses the key to connect to a properly configured authorized access point.

Denial of Service Attacks

A threat to enterprises and service providers delivering hot spot services, denial of service attacks are a threat that can wreak havoc on a large number of users simultaneously. There are various forms of wireless denial of service attacks, but they typically involve flooding a channel or channels with deauthentication or similar packets that terminate all current and attempted client associations to access points.

Detection or Prevention?

Earlier generations of wireless security systems focused on detection. Wireless Intrusion Detection Systems (WIDS) typically rely on signature analysis to provide an alert that a threat is occurring. The WIDS analyzes the information it gathers and compares it to large databases of attack signatures. Essentially, the WIDS looks for a specific attack that has already been documented. As with wire-line detection systems, the solution is only as good as the database of threats. Some systems combine this with anomaly-based detection methods. Anomaly-based systems identify traffic or application content presumed to be different from 'normal' activity on the network or host. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

Wireless Intrusion Detection Systems were appropriate with small numbers of access points and Wi-Fi clients. However, with the exponential growth of Wi-Fi clients and access points within the enterprise and those within range from neighbors outside the premises, WIDS creates an enormous burden for IT and security administrators because they generate a huge number of alerts, many or most of which turn out to be false alarms. As a result, just as the

market turned away from IDS to IPS for wireline security, there has been a rapid shift away from WIDS to a new generation of wireless intrusion prevention systems.

WIDS systems are subject to significant numbers of false positives and false negatives. Because they do not use deterministic techniques, they typically cannot determine whether encrypted APs or NATing APs are on the enterprise network. More importantly, with the widespread use of Wi-Fi in many enterprises, being unable to reliably classify external APs creates huge administrative challenges for IT managers who must deal with alerts from remote sites. In addition, day zero attacks may go undetected, until a new patch or fix is applied. Day zero attacks refer to attacks that exploit vulnerabilities whose detection logic is not supported in the intrusion detection system. Day zero attacks are a huge problem for signature based detection systems, since it is impossible to keep signatures up-to-date with the latest and most sophisticated attacks.

Key Attributes of a Wireless Intrusion Prevention System

Wireless intrusion prevention systems stop attacks before they penetrate and harm the enterprise. WIPS solutions detect each category of attack using deterministic techniques involving a combination of device and event auto-classification, protocol analysis and association analysis. Signatures are only used to provide additional details and are not necessary for detection.

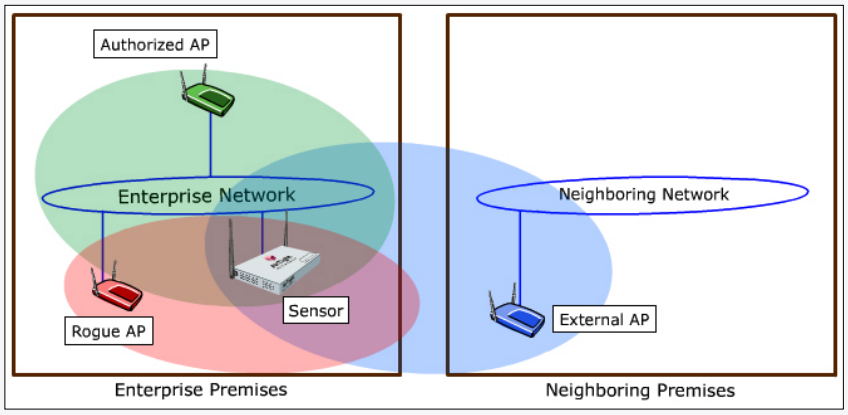
Key attributes of a wireless intrusion prevention system are:

1. **Monitoring/Detection:** All channels in the 2.4 GHz (802.11b, 802.11b/g) and 5 GHz (802.11a) bands should be scanned. It needs to analyze, aggregate, and correlate information reported by different sensors.

2. **Auto-Classification:** With increasing penetration of WLANs, there is a need to accurately and automatically sort harmful activity from the harmless activity in the shared wireless medium. As an example, in organizations with official WLAN infrastructure, the intrusion prevention system must be able to differentiate between authorized, rogue, and external wireless activities. This type of classification minimizes annoying false alarms and volumes of irrelevant alerts from the security standpoint, both of which make the security system unusable.

3. **Prevention:** The WIPS must automatically and instantaneously block harmful wireless activity detected by its wireless sensors. For example, it must block any client from connecting to a Rogue AP or a MAC spoofing AP, prohibit formation of ad-hoc networks, and mitigate any type of DOS attack. Furthermore, it must block multiple simultaneous wireless threats while continuing to scan for new threats.

Prevention of Wi-Fi threats must be carried out with surgical precision to avoid disturbing legitimate WLAN activities. A well implemented WIPS Firewall should not stop traffic on the authorized wireless network or a neighboring Wi-Fi network.



A Wi-Fi Intrusion Prevention System should automatically and precisely classify access points as Authorized, External and Rogue to eliminate false alerts.

4. **Visualization:** The spatial layout as well as materials within the enterprise (walls, columns, windows, furniture, etc.) interact with the radio coverage of the security sensor in a complex way creating a significant gap between rule-of-thumb placement and reality. A systematic, scientific, and scalable RF planning process is therefore required for determining the right placement of access points and wireless sensors. This must be site-specific and not require time consuming manual surveys. Live RF maps should provide real time information on coverage of both authorized Wi-Fi access points and security sensors.

5. **Location:** Physical remediation is a final step in permanently preventing the Wi-Fi threat and requires knowledge of the physical location of these devices. The WIPS Firewall must provide the location co-ordinates of such a device inside and around the perimeter of the enterprise premises without need for any specialized client side software or hardware.

Conclusion

Today, the enterprise air space has become an asset. To protect this asset, wireless intrusion prevention systems are needed to provide 24 x 7 security against unintended and malicious Wi-Fi threats. As recent news events have shown, a lack of robust protection can lead to serious consequences including loss of confidential data, customer trust and brand value. Wireless Intrusion Prevention Systems complement today's wired security solutions and keep the enterprise network safe, whether or not a Wi-Fi network is currently in place.