AirTight
NETWORKS™

Best Practices for Securing Your Enterprise Wireless Network

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

THE LEADER IN WIRELESS INTRUSION PREVENTION

Best Practices for Securing Your Enterprise Wireless Network

Overview

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. As an extension to existing wired infrastructure, Wi-Fi helps companies achieve better customer responsiveness and improvements in the bottom line.

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. In addition, the enterprise wired network itself is subject to unauthorized access without proper precautions. There are five fundamental areas which must be considered when securing the enterprise against wireless threats.

- Creating a wireless security policy
- Securing the enterprise wireless LAN
- Securing the enterprise wireline (Ethernet) network
- Securing corporate laptops from wireless threats when outside the enterprise
- Educate employees regarding the wireless policy

This paper will discuss best practices in all five areas to secure the enterprise network, whether wired or wireless, from unauthorized use and hackers. This should be complemented by strong access control and wireline security policies. This paper assumes that a strong firewall, VPN, a VLAN architecture for multiple user communities and wireline IDS/IPS already are in place. Together, the combination can protect the enterprise from unauthorized use, theft and damage to the company's reputation with customers and partners.

Create a Wireless LAN Security Policy

Much like the security policy that you have in place for wireline access, it's a good idea to begin with a written wireless policy that covers authorized use and security. A good place to start is with some templates that already exist for the specific sections that should be covered. Good places to review documents for a wireless policy include the SANS Institute and CWNP.[1] Typically, security policy documents include the following sections:

- Purpose
- Scope
- Policy

[1] For more information, go to http://www.sans.org/resources/policies/Wireless_Communication_Policy.pdf and http://www.cwnp.com/templates/WLAN_Security_Policy_Template_v1.05.pdf

- Responsibilities
- Enforcement
- Definitions
- Revision History

Background for this document should be thoroughly researched. Most security issues can be traced to oversights or errors in security policy implementation. The following discusses some best practices that you may wish to incorporate into your Wireless LAN Security Policy.

Securing the Enterprise Wireless LAN

Enterprise wireless LAN deployments have skyrocketed in recent years, evolving from guest access in conference rooms, to limited hot zones of connectivity within the enterprise to full coverage throughout the organization. Unfortunately, many of these deployments are still insecure, leaving opportunities for the just plain curious or malicious hackers to try and access confidential enterprise information. Securing a wireless LAN is not hard – industry advances in technology and vendor innovation makes this easier than ever. Following are best practices for securing your enterprise wireless LAN.

Change the Manufacturer's Default SSID to a 'Secure' SSID

Access points come with a standard network name such as tsunami, default, linksys, etc that broadcast to clients to advertise the availability of the access point. This should be changed immediately upon installation.

When renaming the access point SSID, choose something that is not directly related to your company. Do not choose your company name, company phone number or other readily available information about your company that is easy to guess or find on the Internet.

Use Strong Encryption and Authentication

Default settings for most access points do not include any form of security being enabled. This is the most common reason that wireless LANs are hacked or used by unauthorized personnel. When deployed, immediately turn a method of over-the-air security on. For enterprises, it is recommended that the most secure over-the-air encryption and authentication method be used – either IEEE 802.11i or a VPN.

IEEE 802.11i, also known as WPA2 when the access point is certified by the Wi-Fi Alliance, uses IEEE 802.1x for mutual authentication between the client and the network and AES for data encryption. Its predecessor was WPA, an interim form of security certified by the Wi-Fi Alliance while the 802.11i standard was still being ratified. WPA also uses 802.1x for authentication, but TKIP for encryption. While AES is considered the stronger encryption method, it is worth noting that WPA has never been cracked.

802.11i, WPA2 and WPA require the use of a RADIUS server to provide the unique, rotating encryption keys to each client. Multiple manufacturers including Funk Software, Meetinghouse and Cisco provide 802.11i and WPA compliant RADIUS servers. Your existing RADIUS server may be upgradeable – check with your manufacturer.

If 802.11i, WPA2 or WPA cannot be used, a VPN is the next best solution for securing the over-the-air client connection. IPSec and SSL VPNs provide a similar level of security as 802.11i and WPA. Their downside for larger wireless LAN deployments is that all wireless LAN traffic must be funneled to the VPN server, which may create a bottleneck. Also, latency sensitive applications such as wireless VoIP or Citrix may lose connectivity when roaming due to long latencies.

If none of these methods are available, then it is advisable to at least turn WEP on. While WEP is widely known to be easily cracked by hacker's tools available on the Internet, it will at least provide a deterrent to casual snoopers. And, a plan to put a stronger form of security in place should be formed immediately.

Segment User Populations with VLANs

Many different types of users may need to access the wireless LAN network. Order administrators require access to the order entry and shipping systems. Accounting and finance staff require access to accounts receivable and payable as well as other financial systems.

Marketing and sales teams may require access to sales performance data. An access point that supports virtual LANS (VLANS) allows each authorized wireless LAN user to gain entry to only the network resources they need to access. As an example, personnel in shipping and manufacturing might access the wireless network using the SSID 'operations' which provides access only to email and ERP systems. Marketing and sales might access the wireless network using the SSID 'winbusiness' which accesses customer and sales database information. Both of these SSIDs would support strong 802.11i or WPA encryption.

In addition, many corporations may use barcode scanners for inventory tracking or in shipping and receiving. And, as wireless VoIP gains popularity, Wi-Fi phones will become more prevalent. These types of devices often do not support today's strong 802.11i or WPA security, but they will support the less secure WEP encryption. They too can be segregated on a specific SSID which supports WEP and routes traffic to a VLAN which only allows access to the specific database or application they are associated with. This, along with frequent encryption key changes and MAC address control lists, mitigates potential security risks.

Secure Management Access

Not to be forgotten are the management interfaces of the wireless LAN system. The wireless LAN system should support secure, authenticated methods of management. Reconfiguring the access point through the management port is one method a malicious hacker might try to access the corporate network. Wireless LAN systems should provide SNMPv3, SSH (secure

Web), and SSL (secure Telnet) interfaces. Furthermore, the system should be configurable such that management is not possible over-the-air, and ideally a management VLAN is available such that only stations on a specific VLAN can modify the WLAN network settings.

Physically Secure the APs

Finally, the access points should be secured against direct tampering or theft. If possible, access points should be deployed above a suspended ceiling so they are 'out of sight, out of mind', with only the antenna visible. If this is not possible and the access points are physically accessible, management via a local serial port should be disabled or only available via secure access methods. Newer switch-based wireless LAN architectures may also provide additional protection by not storing any information locally in the access point, but keeping it centralized in the wireless switch which can be located in a secured wiring closet.

Physically Monitor Your Exterior Premises

As access point signals extend beyond the perimeter of most buildings, it is possible for someone outside the facilities to connect internally while sitting in a parking lot or across the street. If security patrols or video surveillance is already in use, you may want to alert security personnel to be aware of vehicles or people that seem to be loitering near the building for extended periods of time. In one publicized incident, this is how several hackers were caught trying to steal credit card information from a retail store over the wireless LAN network.

Secure the Enterprise Wired Network Against Wireless Threats

Despite all of the above precautions taken to secure the wireless LAN network, a serious security risk can still exist, exposing the organization to risks and possible regulatory violations, such as Sarbanes-Oxley or HIPAA. Even a "no Wi-Fi" policy is no guarantee of security against these threats. Rogue access points can be brought in by employees. Laptops with embedded Wi-Fi can connect to neighboring networks. Both are real, significant risks. Traditional wireline security methods such as firewalls and VPNs do not detect these types of threats. And once the device is behind the corporate firewall, it is viewed as trusted. In this new era of almost ubiquitous Wi-Fi, the corporate air space itself must be considered an asset and protected.

Deploy Automatic Wireless Intrusion Prevention

The wireless intrusion prevention system (WIPS) provides a trusted 3rd party security system that prevents these Wi-Fi security risks. Much like an intrusion prevention system for wireline systems, a wireless intrusion prevention system both

The Eight Major Categories of Wireless Threats

Common Wireless Threats

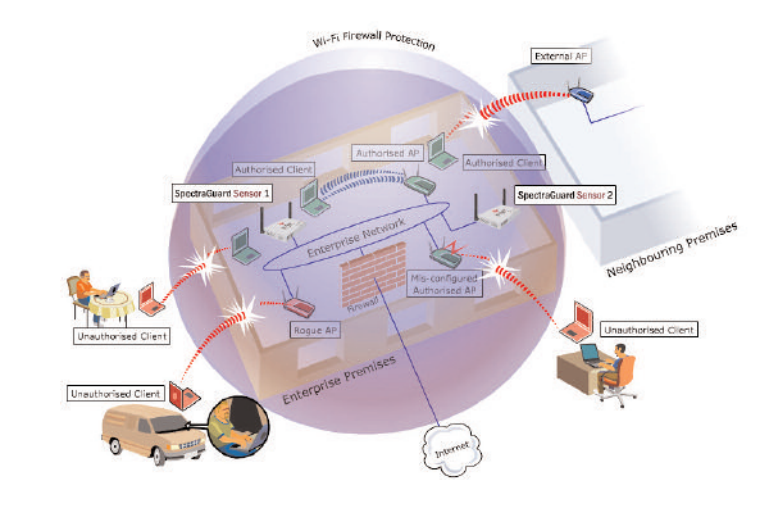
Rogue Access Points

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 detects threats and automatically prevents them. WIPS solutions detect all wireless transmissions over-the-air, classify them and based on rules set up by the administrator can automatically quarantine dangerous devices.

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



A wireless intrusion prevention system (WIPS) provides automatic classification and prevention against wireless threats which cannot be protected against via existing wireline secuirty methods.

Choosing An Overlay vs. Embedded Wireless Intrusion Prevention Solution

Some wireless LAN vendors claim to provide sufficient wireless intrusion prevention capabilities in their infrastructure. While limited protection may be available, several key problems exist with an all-in-one approach.

For companies with a no Wi-Fi policy, or for those enterprises that are not deploying wireless across the entire campus, an integrated solution is not feasible. Corporations need to protect their entire air space, whether or not they have a WLAN as employees are actually more likely to bring in a rogue access point or to connect to neighboring networks in areas

the corporate network if it is reset to system 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), where an authorized wireless network is not installed.

Even for those enterprises with complete wireless LAN coverage, an integrated solution will not provide adequate protection in a number of ways. The attraction of an integrated solution is the assumed lower cost in only deploying a single RF device and pulling a single cable. However, using the access point as a sensor requires that one set of functionality will be diminished or compromised – either client connectivity or continuous monitoring for threats. An access point radio cannot scan all the bands in the channel while simultaneously serving client needs. And, as more and more Wi-Fi devices enter the enterprise and need network connectivity, this approach becomes less feasible.

Secondly, the focus of infrastructure vendors is not on protecting the corporate network. Their priority is to provide reliable, robust wireless client services. The new world of Wi-Fi threats is moving fast with many advances made each month by vendors focused on this arena. Infrastructure vendors are not equipped with the right talent nor time to keep up with this rapidly changing technology area. In many instances, the intrusion prevention capabilities offered by the WLAN are minimal – and disruptive. For example, many solutions claim rogue AP detection and prevention. However, the real truth may be that all APs that are not on the switch network are deemed rogue, when in fact many of them are harmless neighboring networks. Or legacy wireless LANs still operating and in place. And, the prevention techniques are brute force, bringing down not only the rogue AP, but also shutting down the authorized wireless LAN.

Lastly, auditors may enforce separate infrastructure in order to maintain compliance with regulations such as Sarbanes-Oxley or HIPAA. There is ample evidence today that maintaining separation of Ethernet infrastructure and security systems is wise. Security professionals today recommend separate components for Ethernet infrastructure and wireline IDS/IPS to avoid 'the fox watching the hen house.' Similar reasoning applies to wireless networks as well.

Employ Wired Side Port Blocking

If available, wired side port blocking should be employed in

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 danger to any enterprise, 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. Denial of service attacks can be particularly destructive to voice over Wi-Fi applications, completely halting the conversation.

To prevent wireless threats such as these from causing loss of confidential information or harming the company's reputation with customers and partners, the following best practices are recommended.

concert with the wireless intrusion prevention system. Some WIPS manufacturers have integrated their system with wired network equipment manufacturers to complement over-the-air prevention with wired port suppression. In these types of solutions, the WIPS server will communicate with a central management appliance in the wired network and provide information about the rogue access point. Using this information, the management appliance can prevent all traffic from the wired switch port that the rogue AP is connected to.

Use Location Tracking for Physical Remediation

Physical removal of rogue devices is the final step to ensure that the wireless threat is removed. Locating the precise area of the device, however, has not always been easy. Traditionally, handheld analyzers have been used to perform a walk around in the general area that the rogue device is found. However, as wireless propagation can extend quite far, this can be a time consuming proposition, especially for multi-floor sites. Modern wireless IPS solutions provide precise location tracking on specific site floor plans for quick removal of rogue devices.

Perform Regular Wireless Vulnerability Assessments

Regular assessments of the vulnerability of the network to wireless threats should be performed, both by internal and external auditors. Wireless vulnerability assessments can consist of walk arounds with handheld analyzers to look for unknown wireless devices or more structured assessments using tool kits that specifically probe for all different types of threats. The latter is more effective, especially if a wireless intrusion prevention system is in place to automatically quarantine unknown devices. In this case, the wireless vulnerability assessment should be performed regularly to ensure that any new categories of wireless threats are alerted to and contained. If not, then a security hole may exist and the manufacturer should be contacted for software updates.

Securing Your Corporate Assets When Outside the Enterprise

Today's enterprise is amorphous – no single perimeter exists. The enterprise itself is most likely a collection of multiple locations. And these locations extend beyond the corporate addresses to homes, hotels, airports and many other places. With the proliferation of telecommuters and road warriors, mobile devices and ubiquitous Internet access, the enterprise IT manager faces enormous challenges in securing the enterprise from threats while the device is outside the relative safety of the corporation.

Think of the Device as a Self-Contained Enterprise Network

The laptop in particular needs the same protections as an enterprise network. A firewall, VPN and antivirus software all help protect it from the many threats these devices face as they connect to the Internet.

Consider User Authentication and Data Encryption

Like the enterprise network, user authentication for access control and data encryption can significantly strengthen security measures. User authentication can be done via passwords or USB tokens or smart cards. While effective generally, they will not stop someone who removes the hard disk to get to sensitive data. At this point, encryption should be considered. Encryption to work, though, must be automatic and transparent to the user.   If the user must enable it for specific files, it is likely not to be effective due to human failure.

Add Wireless Threat Intrusion Prevention

New threats now arise from the prevalence of Wi-Fi in hotspots, hotels, airports and many other places where business travelers congregate. And wireless users running Windows XP are particularly vulnerable as their client will automatically look to connect to a network name (SSID) that they have successfully connected to before. Articles have even appeared about how easy it is for someone to create a Honey Pot AP on their own laptop and immediately have several surrounding laptops connect to it without their users being aware of the vulnerability. This type of wireless threat, known as an Evil Twin when a malicious hacker creates a website to mimic a log in page to capture user credentials and credit card information, is a rising threat. Additionally, ad hoc networks must also be prevented to ensure that corporate data is not exposed through this type of a connection. Personal wireless firewalls are now also available. Often linked to the security policies of the enterprise's wireless IPS system, they allow the administrator to monitor the threats that the user may have been exposed to and update policies remotely as needed.

Educate Employees About The Wireless LAN Security Policy

More often than not, employees are willing participants in ensuring a secure enterprise network if they are educated about the policies and the potential threats of non-compliance. As an example, most employees would probably not be aware that deploying a wireless LAN access point 'out-of-the-box' endangers corporate network security. Ensure that your company provides multiple opportunities for education – when wireless is first made available to employees and throughout the year.

Conclusion

As the nature of the enterprise has evolved from the paradigm of fixed Ethernet connectivity inside the building to mobile wireless connectivity inside, at home and on the road, the challenge of keeping confidential corporate information secure has soared. Wireless technology has undoubtedly brought incredible productivity gains and organizations must find ways to deploy it securely in order to remain competitive. Fortunately, the wireless industry has also evolved, developing new standards and security solutions both for the wireless infrastructure itself as well as for the wireless perimeter. Protecting today's corporate wireless perimeter, whether inside company offices or while on the road is possible, allowing the enterprise to focus on the business at hand – serving customers and gaining competitive advantage.