White Paper

Five Steps to Securing Your Wireless LAN and Preventing Wireless Threats

Wireless LANs (WLANs) bring incredible productivity and new efficiencies to organizations of all sizes. Advances in WLAN features and capabilities allow organizations to offer the benefits of wireless to their employees without sacrificing security. Properly deployed, WLANs can be as secure as wired networks. This paper discusses the five steps to creating a secure WLAN infrastructure.

CHALLENGE

WLANs have created a new level of productivity and freedom both within and outside the organization. Many applications—both back-office (inventory tracking, mobile printing, and point-of-sale terminals) and front office (e-mail, Internet access, and advanced services such as voice over WLAN and location tracking)—rely on wireless connectivity. However, while productivity has increased, new challenges to security have arisen. By design, wireless signals propagate beyond the physical boundaries of the organization, invalidating the traditional view that the inside of the organization is secure. Signals from unsecured WLANs that extend outside the corporate network can be found and used by unauthorized personnel—or even malicious hackers. Although the wireless medium has specific unique characteristics, essential WLAN security measures are not very different from those required to build strong wired security, and IT administrators can maintain corporate privacy with the proper WLAN security measures employed.

Although IT administrators may already be aware of the proper techniques for securing the WLAN medium itself, they may be surprised to learn that WLAN security alone is not enough to protect the organization. Whether a company has an authorized WLAN or a “no Wi-Fi” policy, it is important to be aware of the vulnerability the hardwired corporate network has to wireless “threats”. The most common is the rogue access point. Eager employees often bring in their own access points—typically consumer-grade and very low cost—to speed wireless connectivity in their department, unaware of the dangers. These rogue access points are behind the firewall and are not detectable by traditional intrusion detection or prevention systems (IDSs/IPSs). Anyone within range of the signal could attach and access the corporate network.

Complicating this situation is the new reality of mobile workers requiring access to the network while on and off premises. Employees regularly use their homes, hotels, airports, and other wireless hotspots to conduct business. These “unmanaged” sites can act as a conduit for threats to the corporate network—laptops risk contracting viruses, spyware, and malware. Wireless clients can exacerbate the problem by connecting to wireless access points or other wireless clients without the user’s knowledge.

SOLUTION

The Cisco® Self-Defending Network (SDN) strategy protects against the new threats to security posed by wireless technologies by dramatically improving the ability of the network to automatically identify, prevent, and adapt to security threats. As part of this strategy, the Cisco Unified Wireless Network provides a comprehensive solution for protecting the wired network from wireless threats and ensuring secure, private communications over an authorized WLAN. Every device in the network—from clients to access points to wireless controllers and the management system—plays a part in securing the wireless network environment through a distributed defense.

Because of its mobile nature, a multilayered approach to security is required. Cisco Systems® recommends the following five-step approach for mitigating risks to the network from wireless threats:

- Create a WLAN security policy.
- Secure the WLAN.

- Secure the wired (Ethernet) network against wireless threats.
- Defend the organization from external threats.
- Enlist employees in safeguarding the network.

This paper discusses best practices in all five areas to secure the network—whether wired or wireless—from unauthorized use through a WLAN link. These practices should be validated against the organization's own risk-management processes and complemented by a strong security implementation. Together, this combination can protect the organization from inappropriate resource use, theft, and damage to the company's reputation with customers and partners. For a comprehensive evaluation of your organization's network security posture, Cisco Advanced Services consultants can analyze your network security in reference to industry best practices, identifying vulnerabilities that could threaten your business. Based on in-depth analysis, Cisco offers recommendations on how to improve your overall network security and prioritizes actions for remediation, which should be complemented by strong access control and security policies.

CREATE A WLAN SECURITY POLICY

Much like the security policy that is in place for wired access, a written wireless policy that covers authorized use and security is a necessary first step. Many templates already exist for the specific sections you should cover (for an example, go to: http://www.cwnp.com/templates/WLAN_Security_Policy_Template_v1.05.pdf). Typically, security policy documents include the following sections:

- Purpose
- Scope
- Policy
- Responsibilities
- Enforcement
- Definitions
- Revision history

Thorough research is essential before creating your security policy—most security breaches can be traced to oversights or errors in security policy implementation. The following sections discuss some best practices that you should incorporate into your WLAN security policy.

SECURE THE WLAN

WLAN deployments have increased significantly in recent years, evolving from guest access in conference rooms to limited "hot" zones of connectivity within the organization to full coverage throughout the organization. Unfortunately, many of these deployments are insecure, leaving opportunities for the curious—or malicious hackers—to try to access confidential information. Securing a WLAN is not difficult; industry advances in technology and the Cisco Unified Wireless Network make it easier than ever. Securing the network is based on extending the Cisco Self-Defending Network strategy, which is based on three pillars: secure communications, threat control and containment, and policy and compliance management. With these three areas in mind, following are best practices for securing your Cisco Unified Wireless Network.

Secure Communications

Secure communications entails both encryption of data and authentication of users to the network. In a wireless network, much like a wired network, these two components do not have to be combined, but for most networks Cisco recommends using both. Exceptions might include hotspot or guest networks, which are discussed in further detail later. In addition, unique characteristics of the wireless medium require adoption of other security techniques to defend the network.

Modify the Default SSID

Access points come with a standard network name such as “tsunami”, “default”, “linksys”, etc. that broadcasts to clients to advertise the availability of the access point. You should change this setup immediately upon installation. When renaming the access-point Service Set Identifier (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. By default, access points broadcast the SSID to any wireless client within range. For some applications, such as hotspots or guest access, this capability allows users to find the network without assistance. However, for corporate networks, you should disable the broadcast to limit those who may be casually looking for an open wireless network.

The Cisco Unified Wireless Network helps ensure that all clients gain access within an operator-set number of attempts. If a client fails to gain access within that limit, it is automatically excluded (blocked from access) until the operator-set timer expires. The operating system can also disable SSID broadcasts on a per-WLAN basis, further reducing the incidence of casual snoopers.

Use Strong Encryption

One of the biggest hurdles to WLAN deployment has been Wireless Equivalent Privacy (WEP) encryption, which is a weak, standalone encryption method. Also, the complexity of add-on security solutions has prevented many IT managers from embracing the benefits of the latest advances in WLAN security. The Cisco Unified Wireless Network bundles security components into a simple policy manager that customizes systemwide security policies on a per-WLAN basis. To enable easy client connectivity, access points are typically not configured by the manufacturer for over-the-air encryption. After deployment, it is easy to forget this step—yet this is the most common way that WLANs are hacked or used by unauthorized personnel. Therefore, you should configure a method of over-the-air security immediately after deployment. Cisco recommends that you use the most secure over-the-air encryption—either IEEE 802.11i or a VPN.

IEEE 802.11i, also known as Wi-Fi Protected Access 2 (WPA2) when the access point is certified by the Wi-Fi Alliance, uses the Advanced Encryption Standard (AES) for data encryption. AES is the current highest standard for encryption, and replaces WEP. You should use WPA2 with AES whenever possible. Its predecessor, WPA, is an interim form of security certified by the Wi-Fi Alliance while the 802.11i standard was still being ratified. WPA uses Temporal Key Integrity Protocol (TKIP) for encryption; TKIP is a form of encryption that delivers significantly improved over-the-air security, while allowing traditional 802.11b clients to be upgraded, preserving customer investment. Although AES is considered the stronger encryption method, it is worth noting that TKIP has never been “cracked”. WPA is recommended as the next-best standard for encryption, and you should use it if you have clients with older networks that can be upgraded. Alternative strategies for securing clients that cannot be upgraded from WEP to TKIP are discussed in the section “Alternative Security Strategies for Business-Specific Clients”.

Note: The 802.11i standard, WPA2, and WPA require the use of a RADIUS server to provide the unique, rotating encryption keys to each client. The Cisco Unified Wireless Network interoperates with the Cisco Secure Access Control Server (ACS) as well as other manufacturers’ 802.11i- and WPA-compliant RADIUS servers. Furthermore, unlike other clients where third-party software might be required to enable IEEE 802.11i capability, Cisco clients ship ready to connect in secure WPA or WPA2 mode to Cisco Unified Wireless Network infrastructure. It is important to note that the personal version of WPA2 and WPA does not require a RADIUS server. Hence, it is recommended for secure home or small office/home office (SOHO) implementations

Cisco Compatible Extensions program helps ensure that a broad range of WLAN client devices interoperate with and support innovative features of Cisco WLAN infrastructure products. As a result, IT managers can deploy WLANs confidently, even when those WLANs serve many types of client devices. Cisco Compatible Extensions is an important initiative that allows delivery of end-to-end performance, RF management, quality of service (QoS), and security capabilities needed in the wireless network. A few of the major security enhancements available through the program include Cisco LEAP, Protected Extensible Authentication Protocol (PEAP), and Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) modes of authentication, along with secure fast roaming with key caching for latency-sensitive applications such as voice over WLAN. Some of these features have been adopted by the standards bodies over time, and Cisco has provided them as they have been ratified.

Because client capabilities are integral to overall network security, Cisco and Intel have collaborated closely within the Cisco Compatible Extensions program. Intel, a strategic alliance partner, has achieved Cisco Compatible status for its Centrino Mobile technology, which is available in many notebook computers. Major notebook suppliers, including Acer, Dell, Fujitsu, IBM, HP, and Toshiba, provide Cisco Compatible notebooks. A complete listing of products in the Cisco Compatible Extensions program is available at: http://www.cisco.com/go/ciscocompatible/wireless

Deploy Mutual Authentication Between the Client and the Network

Another important capability lacking in the original 802.11 standard was mutual authentication between the network and the client. Again, the release of WPA and IEEE 802.11i introduced this capability. Both of these protocols use IEEE 802.1X for mutual authentication between the client and the network.

Alternative Security Strategies for Business-Specific Clients

If you cannot use 802.11i, WPA2, or WPA because the client does not support these encryption and authentication types because of age or lack of driver compatibility, a VPN is the next best solution for securing the over-the-air client connection. A VPN combined with network segmentation using multiple SSIDs and VLANs (described later) provides a robust solution for networks with varied clients. IP Security (IPSec) and Secure Sockets Layer (SSL) VPNs provide a similar level of security as 802.11i and WPA. Cisco wireless LAN controllers terminate IPSec VPN tunnels, eliminating potential bottlenecks from centralized VPN servers. In addition, the Cisco Unified Wireless Network supports transparent roaming across subnets so latency-sensitive applications such as wireless voice over IP (VoIP) or Citrix will not lose connectivity when roaming because of long latencies.

If none of these methods is possible, then you should configure WEP. Although WEP is widely known to be easily compromised by tools available on the Internet, it at least provides a deterrent to casual snoopers. Combined with user segmentation based on VLANs as described later, WEP significantly mitigates the security risk. The Cisco WLAN solution also supports local and RADIUS MAC filtering, which is best suited to smaller client groups with a known list of 802.11 access-card MAC addresses. If using this method, a plan to put a stronger form of security in place should be developed immediately.

Regardless of the wireless security solution selected, all Layer 2 wired communications between Cisco wireless LAN controllers and Cisco Aironet® access points operating with the Lightweight Access Point Protocol (LWAPP) are secured by passing data through LWAPP tunnels. And as a further security measure, disabling is also used to automatically block Layer 2 access after an operator-set number of failed authentication attempts.

Use Identify Networking to Segment Users to Appropriate Resources

Many different types of users need to access the WLAN 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; and marketing and sales teams may require access to sales performance data. The Cisco Unified Wireless Network supports identity networking—a concept whereby WLAN policies are assigned and enforced based upon a wireless client's identity, as opposed to its physical location. With identity networking, wireless devices need to authenticate only once with a WLAN system. Context information follows the devices as they roam, helping to ensure transparent mobility. When the WLAN is associated with a specific VLAN, the user can gain entry to network resources only on that VLAN. As an example, personnel in receiving might access the wireless network using the SSID "receiving", which provides access only to e-mail and enterprise resource planning (ERP) systems. Executives might access the wireless network using the SSID "corp", which accesses financial, customer, and sales database information. Both of these SSIDs support strong 802.11i or WPA encryption.

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

Finally, many organizations are interested in helping guests, partners, and customers access the Internet while at their site. A wireless guest network is an easy way to allow access while eliminating the necessity for IT personnel to authorize individual users. Guest networks use an open security method segregated on a specific SSID that routes traffic to a VLAN that accesses the public Internet only. The SSID in this case is typically broadcast so guests can find it without assistance. User login can be accomplished through a captive portal Webpage so that usage is audited and any terms and conditions must be agreed to before the guest uses the service.

Ensure Management Ports Are Secured

The management interfaces of the WLAN system should support secure, authenticated methods of management. Reconfiguring the access point through the management port is one method a hacker might use to access the corporate network. The Cisco Unified Wireless Network supports Simple Network Management Protocol Version 3 (SNMPv3), Secure Shell (SSH) Protocol (secure Web), and SSL (secure Telnet) interfaces to the Cisco Wireless Control System (WCS). Furthermore, the Cisco WCS is configurable such that management is not possible over the air, and it supports a separate management VLAN so only stations on a specific VLAN can modify the WLAN network settings.

Prevent Network Compromise with a Lightweight Access Point Solution

Cisco lightweight access points do not store encryption or other security information locally, so the network cannot be compromised if an access point is stolen. Furthermore, all access points are automatically authenticated through a X.509 certificate, preventing addition of nonauthorized access points to the network. You should secure access points against tampering to prevent unplanned changes to RF coverage. If possible, deploy them above a suspended ceiling so they are out of sight, with only the antenna visible. To facilitate this type of deployment, Cisco lightweight access points support a Kensington lock interface and connectorized antennas.

Monitor the Exterior Building and Site

Because access point signals extend beyond the perimeter of most buildings, it is possible for someone to connect internally while sitting in a parking lot or across the street. If security patrols or video surveillance are already in use, security personnel should be alerted to be aware of vehicles or people that seem to be loitering near the facility for extended periods of time. The Cisco Unified Wireless Network uses patent-pending Cisco Radio Resource Management (RRM) algorithms that detect and adapt to changes in the air space in real time. You can use Cisco RRM to help mitigate RF propagation beyond the physical building perimeter.

SECURE THE WIRELINE NETWORK AGAINST WIRELESS THREATS

The second pillar of the Cisco Self-Defending Network initiative is threat control and containment, which applies to both the wireless and the wired network. As with other security policies, simply alerting employees to threats is typically not sufficient. A good example is the antivirus policy of not opening e-mail attachments from unknown senders. Most organizations cannot rely on that admonition alone—even a single mistake can cause significant damage to the network, thereby causing significant downtime and lost productivity.

Similarly, wireless threat control and containment are vitally important, especially in an era in which lack of threat control can lead to violations of regulatory controls or legal statutes. Even a “no Wi-Fi” policy is no guarantee of security against these threats. Rogue access points can be brought in by employees, and laptops with embedded Wi-Fi can connect to neighboring networks. Both vulnerabilities are as real as viruses, worms, and spam—and the treats they represent are as significant. Traditional wired security methods such as firewalls and VPNs do not detect these types of threats as they occur over the air, but the Cisco Unified Wireless Network is designed to actively monitor for and prevent these occurrences.

Threat Control and Containment

Integrated Wireless Intrusion Prevention

In the Cisco Unified Wireless Network, access points simultaneously act as air monitors and data forwarding devices. This setup allows access points to communicate real-time information about the wireless domain, including potential security threats to Cisco Wireless LAN controllers, without

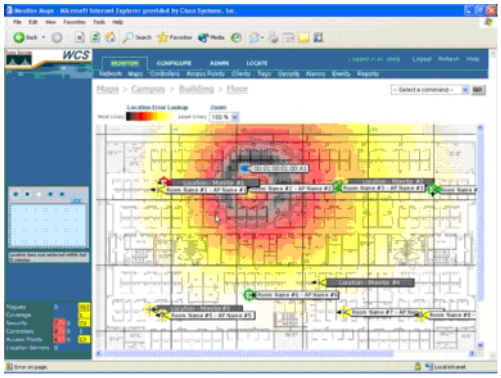
interrupting service. All security threats are rapidly identified and presented to network administrators through the Cisco WCS, where accurate analysis can take place and corrective action can be taken.

If your company has a “no Wi-Fi” policy, you can deploy the Cisco Unified Wireless Network initially as a standalone wireless IPS, and later reconfigure it to add WLAN data service. This scenario allows your network managers to create a “defense shield” around your RF domains, containing unauthorized wireless activity until your organization is ready to deploy WLAN services. Cisco Systems provides the only WLAN system that offers simultaneous wireless protection and WLAN service delivery, helping to ensure complete WLAN protection with no unnecessary overlay equipment costs or extra monitoring devices.

Permanently Remove the Rogue Device with Location Tracking

To ensure that the wireless threat is permanently removed, you must physically remove the rogue device. Traditionally, handheld analyzers have been used in the general area that the rogue device is found. However, because wireless propagation can extend quite far, this proposition can be time-consuming, especially for multifloor sites. The Cisco Location Appliance solution with Cisco WCS can precisely track up to 1500 Wi-Fi-enabled devices such as radio frequency identification (RFID) tags, voice over Wi-Fi phones, laptops, and personal digital assistants (PDAs). (Figure 1). “Precise” refers to the unique ability to define locations where assets or devices can be designated as “in” or “out”. Locations can be an entire campus, a single building, a floor within a building, or a smaller room or coverage area within a floor. With a tracking capability of within a few meters, IT administrators can be immediately alerted of rogue access points and clients, along with their precise location.

Figure 1. Precise Location Tracking of Rogue Access Points and Clients with the Cisco Location Appliance and Cisco WCS



DEFEND THE ORGANIZATION FROM EXTERNAL THREATS

Today’s company has no single perimeter. Mobile device and broadband access have given rise to telecommuters and mobile workers connecting to the organization from homes, hotels, airports, and many other places. The network must be protected from security threats, such as viruses, worms, and spyware, while these mobile devices are away from the office. These security threats disrupt business, causing downtime and continual patching. Policy and compliance management is the final pillar in the Cisco Self-Defending Network strategy to proactively monitor and quarantine malware to maintain network integrity. A compliance program needs to include monitoring to know when system and network policies are violated. Without this, IT administrators cannot know if their security policies are enforced.

Policy and Compliance Management

Provide Similar Security Services to the Mobile Device as the Company Network

The laptop in particular needs the same protections as the company network. Firewalls, VPNs, and antivirus software all help protect it from the many threats these devices face as they connect to the Internet. Tools such as Cisco Security Agent consolidate endpoint security functions such as firewall, intrusion prevention, spyware and adware protection, and more in a single agent. Because Cisco Security Agent analyzes behavior rather

than relying on signature matching, it never needs to be updated to stop a new attack. This “zero-update” architecture provides protection with reduced operational costs and can identify “day-zero” threats. In essence, Cisco Security Agent allows organizations to enforce security policies on individual endpoints.

Like the company network, user authentication for access control and data encryption can significantly strengthen security measures. User authentication can be performed through passwords, USB tokens, or smart cards. Although generally effective, these methods will not stop someone who removes the hard disk to get to sensitive data. At this point, encryption should be considered—but for encryption to work, it must be automatic and transparent to the user. If the user must enable it for specific files, it will likely not be effective because of human failure.

Proactively Ensure Mobile Device Security Policy Compliance with Cisco NAC

Endpoint visibility and control is needed to help ensure that all wired and wireless devices attempting to access a network meet corporate security policies. Infected or vulnerable endpoints need to be automatically detected, isolated, and cleaned.

Network Admission Control (NAC) is a set of technologies and solutions built on an industry initiative led by Cisco Systems. NAC uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from emerging security threats such as viruses, worms, and spyware. Customers using NAC can allow network access only to compliant and trusted endpoint devices and can restrict the access of noncompliant devices. NAC is an important part of the Cisco Self-Defending Network.

Cisco offers both appliance- and architecture-based approaches to NAC that meet the functional and operational needs of any organization, whether it has a simple security policy requirement or requires support for a complex security implementation involving numerous security vendors, combined with a corporate desktop management solution.

Both the Cisco NAC Appliance (Cisco Clean Access) and the Cisco NAC Framework provide security threat protection for WLANs. These solutions enforce device security policy compliance when WLAN clients attempt to access the network, by quarantining noncompliant WLAN clients and providing remediation services to ensure compliance. Both solutions are fully interoperable with the Cisco Unified Wireless Network. Figures 2 and 3 illustrate the Cisco NAC Appliance and Cisco NAC Framework architectures.

Figure 2. Cisco NAC Appliance Architecture for Cisco Unified Wireless Network

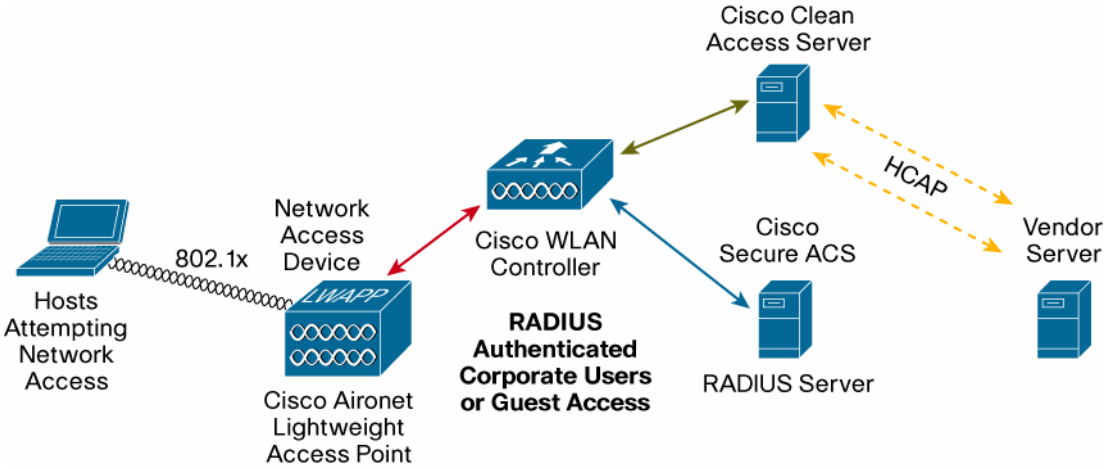
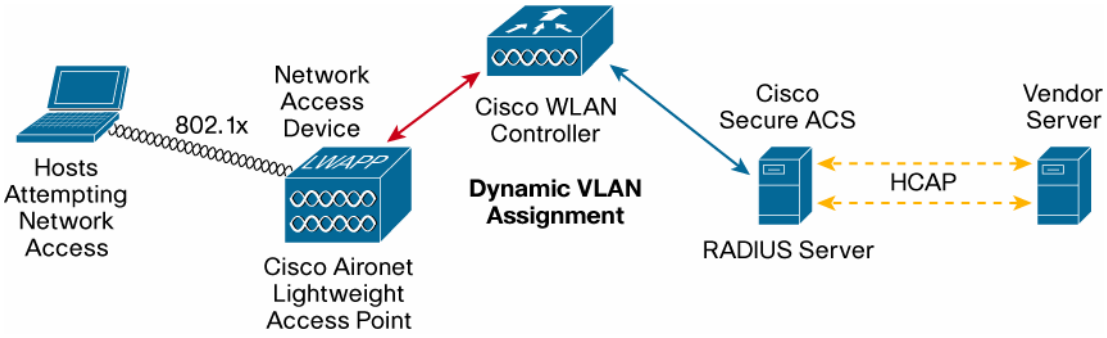


Figure 3. Cisco NAC Framework Architecture for Cisco Unified Wireless Network



ENLIST EMPLOYEES IN SAFEGUARDING THE COMPANY NETWORK

Social engineering is often the most effective tool in helping to secure the network. Most employees are simply not aware of the risks without education—as an example, most people do not realize that the simple act of plugging an access point into an Ethernet jack endangers corporate network security. Employee education—informational posters, or security best practices training (such as password selection and privacy)—has been proven to be effective in helping companies keep their confidential information and networks secure.

CONCLUSION

The organization is no longer defined strictly as the domain within a set of buildings. Mobile devices and technologies have permanently changed the way work is accomplished, allowing connectivity anywhere within the company as well as at home, in airports, hotels, and other Wi-Fi hotspots. With this freedom, new threats arise to the corporate network as wireless signals penetrate beyond walls and devices connect outside the relative safety of the company. To maintain security, proper documentation of a WLAN policy is the first step. Securing the WLAN properly is a must—and the Cisco Unified Wireless Network makes it easy with simple security policies that encompass Layers 1, 2, and 3 for fast deployment.

If no WLAN is currently planned, it is still crucial to prevent against wireless threats such as rogue access points and clients. These threats can open holes in the network, exposing it to hackers and potential theft of confidential information, damage to company reputation, and possible financial and legal penalties. The Cisco Unified Wireless Network can be securely deployed as a wireless IPS solution initially, and then evolved to a WLAN service.

Mobile devices in untrusted environments may pick up new threats. Cisco NAC proactively checks mobile devices for compliance to security policy, providing remediation if necessary and preventing access to the network until compliance is achieved. Finally, employees should be enlisted to help protect network integrity through ongoing training and education. If all these steps are used, the company will significantly mitigate risks to WLANs and from wireless threats. A summary checklist of all the recommended best practices discussed in this paper follows:

- Create a WLAN security policy.
- Secure the WLAN:
  - Modify the default SSID.
  - Use strong encryption.
  - Deploy mutual authentication between the client and the network.
  - Use VPNs or WEP combined with MAC address control lists to secure business-specific devices.
  - Use identity networking in combination with VLANs to restrict access to network resources.
  - Ensure management ports are secured.
  - Deploy lightweight access points as they do not store security information locally.

  - Physically hide or secure access points to prevent tampering.
  - Monitor the exterior building and site for suspicious activity.
- Secure the wired network against wireless threats:
  - Deploy and enable wireless IPSs to prevent rogue access points and other wireless threats—even if you do not have a WLAN.
  - Permanently remove any rogue devices using location tracking.
- Defend against external threats:
  - Equip mobile devices with similar security services as the company network (firewalls, VPNs, antivirus software, etc.).
  - Ensure mobile device security policy compliance with Cisco NAC.
- Enlist employees in safeguarding the network through education.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C78-334982-00 02/06