

Integrity of Information on the Move with the Cisco Secure Wireless Solution

Introduction

The growth of wireless networking has blurred the traditional boundaries between trusted and untrusted networks and shifted security priorities from the network perimeter to information security. The need to secure mobile information and control the wireless environment to prevent unauthorized access must be a priority for maintaining the integrity of corporate information and systems.

Wireless security, especially for Wi-Fi based wireless LANs, must be a priority for IT organizations given the rapid growth of wireless adoption. Wireless LANs have three inherent characteristics that make securing them even more important. The first is that wireless, by definition, transmits via the air and is not contained by physical boundaries like building walls. Thus, existing perimeter security defenses, such as firewalls, are no longer as effective for enforcing policy controls across internal and external boundaries. Secondly, as a standard the 802.11 protocol is well documented and understood and is easily available within the public domain. This pervasiveness increases the ease with which malicious exploits can be attempted. Finally, Wi-Fi operates in the unlicensed frequencies of 2.4 GHz and 5 GHz. Unlike cellular frequencies that require licenses, these unlicensed frequencies are open for use by anyone. While the FCC mandates certain rules of engagement that prohibit aggressive or malicious use, the difficulty in enforcing such rules means most unlawful use of the frequency goes unpunished.

Integrity of Mobile Information

As a basis for any wireless security strategy, IT should focus on protecting sensitive customer, partner, and financial information. The digitalization of information and the ubiquity of IP communications have improved productivity and business processes by making access to information immediate. In an effort to assert control over the availability and integrity of sensitive information, the government and certain industry bodies have defined regulations to help guide businesses on best practices for protecting sensitive data. The number and scope of regulations affecting any single business varies by company size and industry affiliation. Nonetheless, three key regulatory standards emerge as affecting a large number of businesses. Those three regulations include: the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Personal Cardholder Information (PCI) Data Security Standard. Table 1 provides more information on these important standards.

Table 1. Regulatory Requirements

Regulatory	Requirements
Sarbanes-Oxley	All publicly traded companies must: <ul style="list-style-type: none"> • Maintain an adequate internal control structure and procedures for financial reporting • Assess the effectiveness of internal control structures
HIPAA	Requires maintenance of administrative, technical and physical safeguards to: <ul style="list-style-type: none"> • Ensure the integrity and confidentiality of patient information • Protect against threats or hazards, and unauthorized uses or disclosures of patient information
PCI	Any merchant (including electronic) using payment cards, must: <ul style="list-style-type: none"> • Build and maintain a secure network • Protect and encrypt cardholder data • Regularly monitor and test networks, including wireless networks

Although none of these regulations explicitly demands wireless security, the implicit link is clear. Each of these standards calls out the need to protect and control information, whether the information is financial data, sensitive patient records, or credit card transactions. The amount of data transmitted over a wireless infrastructure will continue to grow and must be appropriately encrypted and controlled to avoid unauthorized access. Additionally, the physical wireless environment must be monitored and secured to avoid the possibility of unauthorized access points that create “backdoor access” into corporate systems.

The Cost of a Security Breach

While not all regulations include an enforcement component, several—such as PCI—do. However, the real business impact relates to the cost of a security breach, rather than the enforcement measures that may exist for any specific regulation. Although the immediate threat of fines may increase management’s awareness of the need for tighter security controls, the less tangible cost drivers are far more compelling. Analysis from the Gartner Group claims that the direct cost of a security breach of a single customer record is from \$90 up to \$1,500.¹ Additional research published by Information Systems Security indicates that the impact of a public security breach on a company’s market capitalization can be significant. The study estimated that a drop in company share price attributed to a public security incident is 2.7 percent over one day, increasing to 4.7 percent over three days.²

The costs associated with a security breach of customer or financial data include the following:

- Regulatory fines
- Cost of third-party security audits
- Compensation to customers or partners
- Loss of customer confidence resulting in a decrease in future revenues
- Damage to the corporate brand
- Decrease in investor confidence
- Drop in market capitalization

¹ Data Protection Is Less Costly Than Data Breaches, Gartner Group, 16 September 2005

² The Financial Impact of IT Security Breaches: What Do Investors Think?, Information Systems Security, March/April 2003.

Limiting Exposure with the Cisco Secure Wireless Solution

Cisco® helps companies meet their data security requirements through the Cisco Self-Defending Network strategy. The self-defending network is Cisco's long-term strategy to protect an organization's business processes by identifying, preventing, and adapting to threats from both internal and external sources. This protection helps organizations take better advantage of the intelligence in their network resources, thus improving business processes and cutting costs.

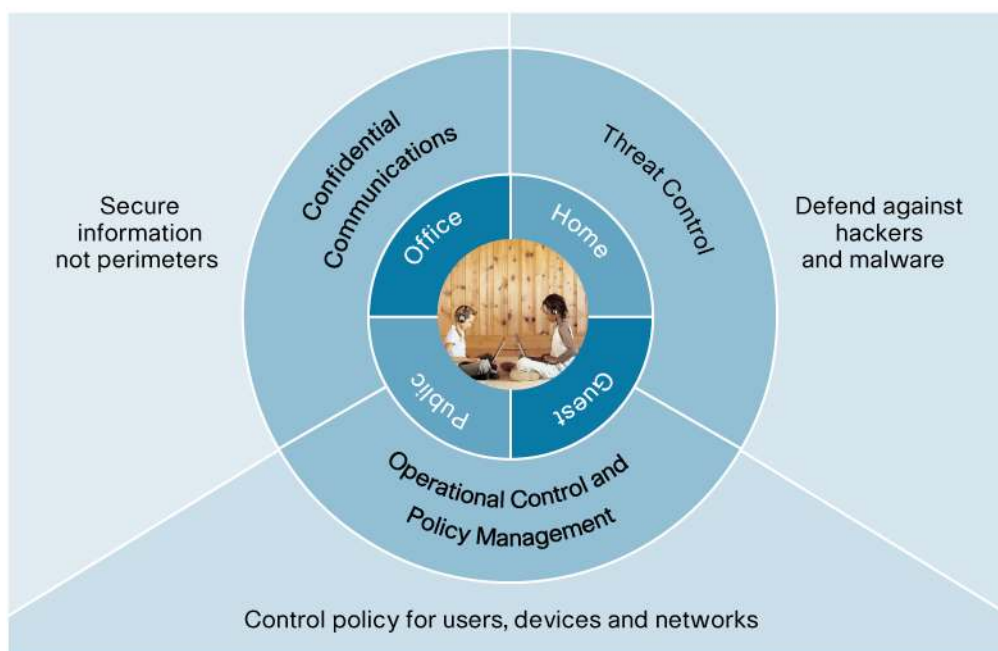
Characteristics of Cisco Self-Defending Network security solutions include:

- The integration of security throughout all aspects of the network
- Collaborative processes between the various security and network elements
- The ability of the network to adapt to new threats as they arise

The self-defending methodology provides businesses with guidelines for creating a secure communications infrastructure and helping the business to achieve its compliance goals. To address wireless security requirements, Cisco recommends companies take an architectural approach to designing and building the wireless network.

The Cisco Secure Wireless Solution is a comprehensive security framework that combines confidential communications for information in transit, policy control for a variety of users and deployment scenarios, and a robust threat defense capability to protect information and systems from wireless threats (see Figure 1). It delivers a comprehensive architecture that integrates the inherent security capabilities of the Cisco Unified Wireless Network with relevant security solutions, including the Cisco Network Admission Control (NAC) Appliance, the Cisco ASA 5500 Series Firewall with Cisco Intrusion Protection System (IPS) software, and the Cisco Security Agent, as well as many other components.

Figure 1. The Security Framework of the Cisco Secure Wireless Solution



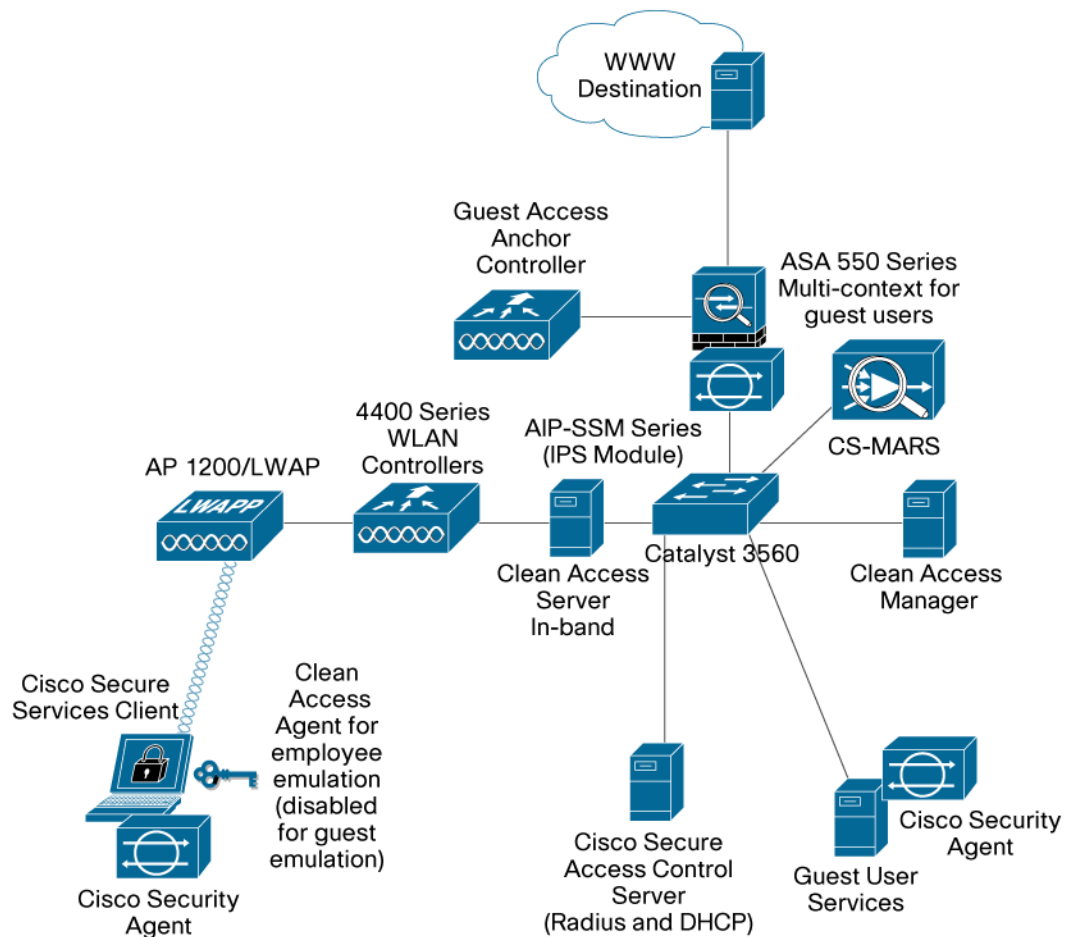
The Components of the Secure Wireless Solution

The Cisco Secure Wireless Solution is an end-to-end architecture that integrates key security and wireless solutions to deliver standards-based, industry-leading network protection (see Figure 2). The architecture combines both wired and wireless security services to present a unified suite of security capabilities that not only deliver a more robust threat defense but also lower the total cost of implementing and maintaining a secure wireless network.

Critical features of the Cisco Secure Wireless Solution include:

- Unified wired and wireless intrusion protection system/intrusion detection system (IPS/IDS)
- Client validation, posture assessment, and remediation
- Wireless single sign-on and 802.1X integration
- Granular control for secure guest access
- Host intrusion prevention
- Rogue detection via automatic RF monitoring
- Wireless security management

Figure 2. Architectural Overview of the Cisco Secure Wireless Solution



Unified Wired and Wireless Intrusion Prevention

Featured Products

- Cisco Intrusion Prevention System Module (AIP-SSM)
- Cisco ASA 5500 Firewall
- Cisco Wireless LAN Controller

The Cisco Secure Wireless Solution integrates wired and wireless intrusion detection and prevention to mitigate the threat from hackers and malicious code. The network inspects traffic flows from the IP layer up to the application layer (L3 to L7) and monitors for potentially harmful signatures or suspicious application behavior. In the event that a signature is detected, the wired IPS solution will alert the wireless LAN controller that the signature is originating from the wireless network. The wireless LAN controller will then issue a client shun request to the identified client and physically block its association with the access point. This integration of wired and wireless solutions offers zero-day alerting and response to potential viruses, malware and suspect signatures.

Client Posture Assessment and Remediation

Featured Products

- Cisco NAC Appliance
- Cisco Wireless LAN Controller

The Cisco Secure Wireless Solution has the ability to validate the identity of the user and device and enforce granular policies to ensure that user or device is supporting the latest antivirus and spyware protection software. In the event that a client is not up-to-date, the solution will quarantine the client, isolating it from the rest of the network, until such time as the user (or administrator) can resolve the problem. This tight integration between the Cisco NAC Appliance and the Cisco Unified Wireless Network ensures that the wireless client adheres to the latest security policies and does not infect the network with malware obtained from external networks.

Wireless Single Sign-On

Featured Products

- Cisco NAC Appliance
- Cisco Wireless LAN Controller
- Cisco Secure Services Client
- Cisco Secure Access Control Server (ACS)

The solution also leverages the 802.1X authentication capabilities of the Cisco Secure Services Client to simplify the wireless user experience by allowing single sign-on to the wireless network domain as well as to the NAC Appliance (for posture assessment). This feature streamlines the user experience and serves to consolidate accounting and administration while improving password management. The combination of 802.1X authentication and posture assessment secures the connection and protects the network from malware while being noninvasive to the user.

Secure Guest Access

Featured Products

- Cisco Wireless LAN Controller
- Cisco ASA 5500 Series Firewall
- Cisco NAC Appliance (optional)

Businesses are experiencing increasing demand to provide network connectivity to a variety of nonemployees, including but not limited to visitors, contractors, consultants, and partners. Wireless is a perfect guest access medium given the ubiquity of Wi-Fi within notebooks. The Cisco Secure Wireless Solution offers two levels of guest access. The baseline guest capability uses a secure tunnel from the controller within the network to a guest controller in the unsecured network area to direct guest traffic directly outside of the enterprise network. Additionally, the guest controller offers a customizable Web interface for user login and liability clauses and has a lobby ambassador feature to support variable login permissions on a per-user basis.

For more advanced guest services, including the ability to define role-based access and conduct client posture assessment and remediation, the Cisco Secure Wireless Solution incorporates the Cisco NAC Appliance to supplement the inherent capabilities of Cisco wireless LAN controllers. Using the Cisco ASA Firewall family of products, the solution can add granular network traffic policies and enforcement for unparalleled content control.

Endpoint Wireless Use Controls

Featured Products

- Cisco Security Agent

By definition, a mobile client often connects to both trusted and untrusted networks. While much of the existing IT focus is on protecting the internal network from exposure to attacks brought in by these mobile clients, the client itself must also be protected. The Cisco Secure Wireless Solution incorporates wireless acceptable use capabilities to enforce client connection policies to better protect the corporate device while connecting outside of the trusted network. The Cisco Security Agent also provides Day Zero attack protection, and has the ability to enforce specific wireless policies including the following:

- Disabling the wireless network interface card (NIC) when connected to the wired network
- Disabling of wireless ad hoc connections
- Enforcement of service set identifier (SSID) association policies
- Enablement of VPN during network connections that are not trusted

Rogue Detection and Containment

Featured Products

- Cisco Unified Wireless Network
- Cisco Location Appliance

A critical component of any wireless security strategy is the use of RF monitoring capabilities to gain visibility into the wireless environment to prevent unauthorized use.

Because so many employees are attracted to the freedom of wireless connectivity and the low cost of consumer grade access points, rogue access points have become a common problem for many businesses. Most companies take an aggressive approach toward building a secure transport for wireless connections, and their approach is generally based on the Wi-Fi Protected Access (WPA) and WPA2 industry standards. However, few companies fully understand the requirement for comprehensive RF monitoring. RF monitoring is needed to gain visibility into the wireless environment and ensure that rogue access points or malicious activity from external (or internal) parties is not creating backdoor access to the network, leaving corporate systems exposed.

The Cisco Secure Wireless Solution integrates RF monitoring directly into the access points and offers continual, 24/7 monitoring to identify, locate, and contain unauthorized wireless activity. This capability is essential for the protection of sensitive information as part of any business compliance initiative.

Wireless Security Management

Featured Products

- Cisco Wireless Control System
- Cisco Security MARS

As with any security solution, intuitive management tools are a prerequisite to maintaining a secure network. The Cisco Secure Wireless Solution uses the Cisco Wireless Control System (WCS) for wireless LAN planning, configuration, and management. Cisco WCS provides a foundation that allows IT managers to design, control, and monitor enterprise wireless networks from a centralized location, simplifying operations and reducing total cost of ownership. WCS will alert network managers to security threats and provide a graphical view of the network, including the location and threat level of rogue

access points. In combination with WCS, the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) recognizes and correlates real network attacks and provides actionable guidelines on how to stop them. The combination of these management capabilities provides the most comprehensive and intuitive management framework of any wireless security architecture available today.

In addition to the features already outlined, the Cisco Secure Wireless Solution incorporates industry-leading features for enhanced security. Cisco has led the industry in the development of management frame protection (MFP), a technology that increases the level of encryption for data in transit by encrypting the management frames of the 802.11 packet. When deployed in combination between the client and the infrastructure, MFP drastically reduces the threat of protocol-based attacks, including man-in-the-middle attacks.

As the number of client devices accessing the network skyrockets, Cisco recognizes the importance of client management and security. Through the Cisco Compatible Extensions program, Cisco is able to bring security features such as MFP to companies by working directly with Wi-Fi silicon manufacturers to uniformly embed specific features into the device. The support for specific security features improves the overall network security and ensures simple, secure connectivity between client and infrastructure. In parallel, Cisco continues to work with the standards bodies to bring the same security features to market in an open, standards-based way.

Integrated Services and Support

To remain competitive in business, companies today need to quickly address unexpected changes, opportunities or threats that come their way. Cisco Services and its WLAN and Security specialized partners can help your organization to thrive today's regulatory requirements.

Our Security and WLAN experts leverage Cisco proven tools and best practices methodologies, and can help you build an end-to-end secure WLAN infrastructure, creating a secure and flexible solution that addresses business challenges like PCI compliance, security and risk management.

Summary

Wireless networking is changing the way IT approaches network security. The physical characteristics of wireless and the experience of mobility mean information moves more freely, with little regard to physical boundaries. Additionally, businesses are relying more heavily on the digitalization of information for improved productivity and are now faced with a rising tide of regulatory requirements put in place to protect the integrity of this information. Providing adequate control and security for all information, but especially customer and financial data, is at the heart of many regulatory requirements, including Sarbanes-Oxley, HIPAA, and PCI.

Cisco is delivering the Cisco Secure Wireless Solution as the preferred architecture for helping to ensure the integrity of information and IT systems. Cisco is the only technology provider to combine industry-leading wireless security protocols such as WPA and WPA2 with best-in-class security solutions such as the Cisco NAC Appliance, Cisco ASA firewalls, and the Cisco Security Agent. The result is a security solution that not only ensures the protection of financial, customer, patient, and credit card data, but also allows IT to support business regulatory compliance initiatives with confidence.

For more information visit:

- Cisco Wireless Security Solutions: <http://www.cisco.com/go/wirelesssecurity>

- Cisco Unified Wireless Network: <http://www.cisco.com/go/unifiedwireless>



Americas Headquarters
Cisco Systems, Inc.
170 West Tauman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 520-4000
800 653-1715 (toll free)
Fax: 408 527-0689

Asia Pacific Headquarters
Cisco Systems, Inc.
155 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7798

Europe Headquarters
Cisco Systems International BV
Hertofbergpark
Hertofbergweg 13-19
1101 CH Amsterdam
The Netherlands
www.europe.cisco.com
Tel: +31 20 600 020 0/91
Fax: +31 20 657 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Ring logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access, Register, Abroad, EPC, Catalyst, CSDA, CCIP, CCIE, CCIP/CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Cisco Voice/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IQS, iPhone, IPTV, IQ Director, the IQ logo, IQ Net, Roadshow, Scorecard, Quick Study, iQoS, iStream, iStocks, iMeeting Place, iMGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RaptorLIX, ScriptShare, SlideCast, SMARTnet, StackWise, The Router, Way to Increase Your Internet Quotient, and Thousand are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (07012)