Q&A

CISCO WIRELESS SECURITY SUITE

OVERVIEW

Q. What is the Cisco® Wireless Security Suite?
A. The Cisco Wireless Security Suite is an enterprise-ready, standards-based, wireless LAN (WLAN) security solution for Cisco Aironet® wireless products and Cisco Compatible Extensions client devices. This solution provides network managers with robust wireless security services that offer freedom and mobility to end users while maintaining a secure network environment.

Q. Does the Cisco Wireless Security Suite support the Cisco Structured Wireless-Aware Network (SWAN)?
A. Yes. The Cisco Wireless Security Suite fully supports Cisco SWAN. Cisco SWAN provides the framework to integrate and extend wired and wireless networks to deliver the lowest possible total cost of ownership for companies deploying WLANs. Cisco SWAN extends “wireless awareness” into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations have come to expect from their wired LANs. Cisco SWAN allows enterprise and service provider network managers to deploy, operate, manage, and secure several, hundreds, or thousands of access points across numerous industries or deployment scenarios. For more information about Cisco SWAN, visit: http://www.cisco.com/go/swan

FEATURES AND BENEFITS

Q. What benefits does the Cisco Wireless Security Suite provide?
A. The Cisco Wireless Security Suite provides scalable, centralized security management that closely parallels the security available in a wired LAN. This enterprise-class solution mitigates sophisticated passive and active WLAN attacks and supports dynamic encryption keys to protect the privacy of transmitted data. Quality of service (QoS) and mobility are integrated into the Cisco Wireless Security Suite framework to enable a rich set of enterprise applications.

Q. What are the features of the Cisco Wireless Security Suite?
A. Features of the Cisco Wireless Security Suite include:

• Strong, mutual authentication and dynamic per-user, per-session, encryption key management via support for IEEE 802.1X

• Data encryption using Temporal Key Integrity Protocol (TKIP), Wired Equivalent Privacy (WEP) and, in 2004, Advanced Encryption Standard (AES)

• Strong TKIP encryption enhancements such as message integrity check (MIC), per-packet keys via initialization vector hashing, and broadcast key rotation

• Support for the broadest range of 802.1X authentication types, client devices, and client operating systems on the market

• Mitigation of network attacks

• Full support for the Wi-Fi Alliance security standard Wi-Fi Protected Access (WPA)
Q. Is the Cisco Wireless Security Suite a component of the Cisco Self-Defending Network?
A. Yes. The Cisco Wireless Security Suite is a component of the Cisco Self-Defending Network. The Cisco Self-Defending Network strategy describes the Cisco vision for security systems. The Cisco strategy of the Self-Defending Network brings together Secure Connectivity, Threat Defense, and Trust and Identity Management with the capability of infection containment and rogue device isolation in a single solution. For more information about the Cisco Self-Defending Network, visit:

WPA
Q. What are WPA and the Wi-Fi Alliance?
A. WPA was introduced in 2003 by the Wi-Fi Alliance, a nonprofit international association that certifies interoperability of WLAN products based on IEEE 802.11 specifications. WPA provides enhanced, interoperable, standards-based security for WLANs. WPA includes portions of the proposed IEEE 802.11i security standard that can be installed as a software and firmware upgrade on existing Wi-Fi Compliant IEEE 802.11 hardware. WPA was designed to be forward-compatible with the IEEE 802.11i standard. It includes support for IEEE 802.1X and the IEEE 802.11i version of TKIP, which Cisco refers to as WPA TKIP to differentiate it from Cisco TKIP.

Q. Does the Cisco Wireless Security Suite support WPA?
A. Yes. The Cisco Wireless Security Suite provides full support for WPA.

Q. Will the Cisco Wireless Security Suite support IEEE 802.11i, WPA2, and AES?
A. Yes. In 2004, the Cisco Wireless Security Suite will also support IEEE 802.11i and WPA2. IEEE 802.11i is the IEEE standard for WLAN security that was ratified in June 2004. WPA2 is the successor to WPA. Both 802.11i and WPA2 include AES as an alternative to TKIP.

Q. Should I use Cisco TKIP or WPA TKIP on my client devices and access points?
A. Some client devices and adapters, such as Cisco Compatible devices and Cisco Aironet client adapters, support both Cisco TKIP and WPA TKIP. Other client devices and adapters support only WPA TKIP. Some legacy Cisco Aironet adapters may support only Cisco TKIP.

With the Cisco Wireless Security Suite, both Cisco TKIP and WPA TKIP algorithms are available on Cisco Aironet access points and Cisco and Cisco Compatible WLAN client devices. Although Cisco TKIP and WPA TKIP do not interoperate, Cisco Aironet access points can run Cisco TKIP and WPA TKIP simultaneously when using multiple VLANs. System administrators will need to choose one set of TKIP algorithms to activate on enterprise client devices, because clients cannot simultaneously support both sets of TKIP algorithms. Cisco recommends that WPA TKIP be used for client devices and access points wherever possible.

COMPONENTS
Q. What are the components of the Cisco Wireless Security Suite?
A. The Cisco Wireless Security Suite is included with all Cisco Aironet wireless products and Cisco Compatible Extensions client devices. IEEE 802.1X mutual authentication requires a RADIUS or authentication, authorization, and accounting (AAA) server and Extensible Authentication Protocol (EAP) types. The Cisco Secure Access Control Server (ACS) or Cisco CNS Access Registrar® is recommended. The Cisco Wireless Security Suite supports several EAP types, including Cisco EAP (LEAP), EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), EAP-Transport Layer Security (EAP-TLS), Protected EAP (PEAP), EAP-Tunneled TLS (EAP-TTLS), and EAP-Subscriber Identity Module (EAP-SIM).

Q. What is IEEE 802.1X?
A. IEEE 802.1X is a port-based security standard (set by the IEEE 802.1 Working Group) for network access control. IEEE 802.1X for IEEE 802.11 takes advantage of standard protocols such as EAP and RADIUS to provide centralized user identification, authentication, dynamic key management, and accounting. This protocol is compatible with wireless roaming technologies, and works between supplicants and authenticators. Authentication and authorization are achieved with back-end communication to an authentication server, such as Cisco Secure ACS.
Q. What is EAP?
A. EAP is a flexible authentication protocol (specified in RFC 2284) that typically rides on top of another protocol such as IEEE 802.1X, RADIUS, or TACACS+. EAP enables the support of new, advanced user authentication methods that allow the authenticator (an Ethernet solution such as a switch, or a WLAN infrastructure device such as an access point) to serve as the user authentication carrier between the client supplicant (software on the client device that is trying to connect to the network) and the authentication server (such as a RADIUS server that supports the appropriate EAP type). Examples of EAP types include:

- Cisco LEAP—802.1X EAP authentication type developed by Cisco Systems to provide dynamic per-user, per-session encryption keys.
- EAP-FAST—Publicly accessible IEEE 802.1X EAP type developed by Cisco Systems to support customers who cannot enforce a strong password policy and wish to deploy an 802.1X EAP type that does not require digital certificates. EAP-FAST supports several user and password database types, supports password expiration and change, and is flexible, easy to deploy, and easy to manage.
- PEAP—802.1X EAP authentication type that takes advantage of server-side EAP-TLS and supports several different authentication methods, including logon passwords and one-time passwords (OTPs).
- EAP-TLS—802.1X EAP authentication algorithm based on the TLS protocol (RFC 2246). TLS uses mutual authentication based on X.509 certificates.
- EAP-Message Digest 5 (MD5)—User name and password method that incorporates MD5 hashing for more secure authentication.
- EAP-Generic Token Card (GTC)—One of the defined EAP types in RFC 2284, supports authentication using OTPs and other criteria.

DEPLOYMENT

Q. What is the deployment advantage of the Cisco Wireless Security Suite?
A. In order to deploy large-scale enterprise WLANs, network administrators need scalable, problem-free security administration that does not increase the burden on the IT staff. The Cisco Wireless Security Suite easily integrates with an existing network, and is available on easy-to-install Cisco Aironet products. With the Cisco Wireless Security Suite’s security features properly configured and activated, network administrators can feel confident that company data will remain private and secure.

Q. Who can deploy the Cisco Wireless Security Suite?
A. Small businesses to large-scale enterprise multinational companies can deploy the Cisco Wireless Security Suite within any Cisco Aironet deployment.

Q. Is the Cisco Wireless Security Suite available today?
A. Yes. The Cisco Wireless Security Suite with IEEE 802.1X and TKIP has been available from Cisco since November 2001, with support for Cisco LEAP available since December 2000. Network managers can implement the Cisco Wireless Security Suite solution to meet their specific network configuration requirements using an EAP type of their choice.

Q. Where can I learn more about deploying the Cisco Wireless Security Suite?
A. Several Cisco Wireless Security Suite deployment guides are available. Please visit the Cisco Aironet Technical References website to view these documents.

Q. Where can I learn more about deploying secure WLANs?
A. Read the following documents to learn more about deploying secure WLANs:

- Wireless LAN Security White Paper
- Cisco Aironet Technical References
Q. Where can I learn more about WLAN security?
A. Please read the Cisco Aironet WLAN Security brochure to learn more about WLAN security.

ATTACK MITIGATION
Q. What network attacks are mitigated by the Cisco Wireless Security Suite?
A. The Cisco Wireless Security Suite mitigates several network attacks, including man-in-the-middle, authentication forging, weak key attacks, packet forgery, and brute force attacks when PEAP, EAP-TLS, EAP-FAST, or Cisco LEAP are used with TKIP or AES. It is important to note that Cisco LEAP requires strong passwords.

Q. Where can I learn more about WLAN network attacks?
A. Read the Cisco Aironet Wireless LAN Security Overview—Temporal Key Integrity Protocol section as well as the WLAN deployment documents listed above.

FOR MORE INFORMATION
For more information about the Cisco Wireless Security Suite, visit:
http://www.cisco.com/go/aironet/security
For more information about Cisco SWAN, visit:
http://www.cisco.com/go/swan
For more information about Cisco Aironet products, visit:
http://www.cisco.com/go/aironet
For more information about Cisco Compatible client devices, visit:
http://www.cisco.com/go/ciscocompatible/wireless
For more information about Cisco Secure ACS, visit:
http://www.cisco.com/go/acs
For more information about Cisco CNS Access Registrar, visit: