

Technology Application Support

Wireless Security Posture Assessment

Wireless Security Posture Assessment is designed to strengthen the security state of your wireless infrastructure by identifying risks and points of exposure, and recommending solutions for improvement.

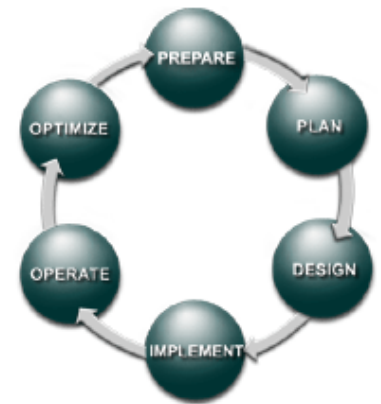
SERVICE OVERVIEW

The challenges of keeping your network infrastructure secure have never been greater or more important to your business. To help ensure your business is protected, security must be an intrinsic part of the network, implemented throughout your environment to address a range of security threats.

To help you mitigate security threats and meet your goals for network productivity and total cost of ownership, Cisco® Advanced Services for Network Security offers expert advice and services to support the network as you plan, design, implement, operate, and optimize a network security solution. Unique from Cisco Systems® is a complete services offering in which security is integral to the network.

Planning Network Security

As the first step in planning network security, Cisco can provide you with a comprehensive evaluation of your organization's network security posture. Delivered by security experts with extensive field experience, the Security Posture Assessment (SPA) provides a snapshot of the security state of your network by conducting a thorough assessment of your network devices, servers, desktops, and databases. Cisco experts analyze the effectiveness of your network security in reference to recognized industry best practices, revealing the relative strengths and weaknesses of your environment. In addition, they document identified vulnerabilities that could threaten your business.



Wireless Security Posture Assessment

The Wireless Security Posture Assessment (Table 1) evaluates the security posture of your organization's wireless network to identify risks and points of exposure associated with a wireless deployment. Cisco experts analyze the wireless technology architecture and configurations to identify authorized and unauthorized access points and recommend solutions to strengthen the security state of the wireless infrastructure.

Cisco experts begin by surveying your premises to discover and map all available access points. By comparing the access points found as well as data gathered during the site survey against a list of authorized devices, Cisco is able to identify possible rogue devices. After completing an inventory of access points, Cisco engineers compare the wireless network architecture and configuration to industry best practices, documenting known vulnerabilities and threats.

Moving outside your buildings, engineers use sophisticated wireless antennas to seek wireless LAN (WLAN) traffic leaking from buildings. If necessary, engineers move into controlled areas of the building to continue seeking WLAN traffic. After traffic is discovered, engineers determine the encryption and authentication method used, in an attempt to gain access to the LAN segment. Table 1 details the activities, deliverables, and benefits of the Wireless Security Posture Assessment.

Table 1 Deliverables, Activities, and Benefits of the Wireless Security Posture Assessment

Deliverables and Activities	Benefits
<p>Identify, validate, and confirm the presence of vulnerabilities on your IP WLAN network. Activities typically include:</p> <ul style="list-style-type: none"> • Examine the wireless access point configurations and compare them against recommended security practices • Find WLAN traffic leaking from customer buildings by deploying sophisticated wireless antennas • Map signal coverage by using global positioning satellite (GPS) technology to plot the area if WLAN traffic is detected • Check for signal visibility and strength in public areas inside the buildings, and in controlled areas of the buildings if necessary, if no WLAN traffic is detected outside the buildings • Determine if wired equivalent privacy (WEP) encryption is enabled or if wireless traffic is being transmitted without encryption 	<p>Mitigate network security threats</p> <ul style="list-style-type: none"> • Protects proprietary information by identifying the potential for unauthorized access and recommending action to help reduce vulnerability • Helps you stay current on new security threats by providing information on vulnerabilities and changes that need to be made (it is recommended that a Security Posture Assessment be performed periodically, depending on the complexity of your network) • Supports the design of an infrastructure that will effectively respond to threats by identifying holes and gaps, and recommending action to improve security • Preserves the security state of the network while integrating new products and technologies into the existing architecture by revealing gaps and vulnerabilities resulting from their integration • Validates your security requirements against industry practices by identifying gaps between the security state of your network and recommended practices, and making recommendations to help resolve the gaps • Protects network security following network expansion by identifying new gaps that may result from network expansion and providing recommendations for addressing them <p>Improve organizational productivity</p> <ul style="list-style-type: none"> • Helps prevent disruption of services to customers and employees due to security breaches by removing vulnerabilities and reducing the number of attacks • Helps increase the productivity of network security and IT staff by providing an influx of expertise through engineers solely focused on studying vulnerabilities <p>Reduce total cost of ownership for network security infrastructure</p> <ul style="list-style-type: none"> • Can prevent the need for costly redesign of the network security infrastructure by providing information needed to develop a sound design, such as which services are running on the network and where vulnerabilities exist • Helps reduce time and resources needed to keep up with potential sources of vulnerability by providing a team of engineers dedicated to understanding new vulnerabilities and how they affect the network, who can periodically assess the security state of your network
<p>Confirm the vulnerability on identified security weaknesses to more effectively determine the level of unauthorized access. Activities typically include:</p> <ul style="list-style-type: none"> • Attempt to decipher WEP • Attempt to obtain customer IP addresses and evaluate the security of the access points 	
<p>Analyze and present IP WLAN assessment results. Activities typically include:</p> <ul style="list-style-type: none"> • Identify critical deficiencies by analyzing and reviewing data and comparing wireless assessment results with current operational requirements • Analyze and review data; compare results of the wireless assessment with recommended security practices and specific policies, controls, or operational requirements of concern to the organization • Present security vulnerability and recommendations summary 	
<p>Develop IP Wireless LAN Security Vulnerability and Recommendations report. This deliverable typically includes:</p> <ul style="list-style-type: none"> • The most critical assessment findings • Data and statistics regarding individual systems and vulnerabilities • Recommendations for improvement 	



AVAILABILITY

Wireless Security Posture Assessment is available globally. To obtain the most current availability status, contact your Cisco representative.

SUMMARY

Cisco Systems® offers various services programs to help accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business.

ORDERING

The Wireless Security Posture Assessment is an a-la-carte offering, available without a subscription to any other service.

FOR MORE INFORMATION

For more information about the Wireless Security Posture Assessment or other Cisco Services, visit www.cisco.com/en/US/products/svcs/ps11/services_segment_category_home.html or contact your Cisco service account manager.

**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 Web site 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

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, and Cisco IOS are registered trademarks or 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. (0402R)

Printed in the USA