

Automated Wireless Security Vulnerability Assessment

Using the Cisco Wireless Security System to Analyze Network Security

Background

As wireless networks are globally deployed across enterprise locations, wireless network administrators must work to ensure that proper configurations and security controls are applied to protect both the wired and wireless network from malicious attacks and threats. Identifying, monitoring, and understanding security alerts, and taking the time to manually audit security and configuration settings, can be time consuming and difficult in large, distributed deployments. Network administrators are looking for tools to prioritize alarms, automate security auditing, and consolidate the information required to meet reporting and regulatory requirements.

Solution Overview

Cisco® Wireless Control System (WCS) is the industry's leading platform for wireless LAN planning, configuration, management, and mobility services. It provides a powerful foundation that allows IT managers to design, control, secure, and monitor enterprise wireless networks from a centralized location, simplifying operations and reducing total cost of ownership. Cisco WCS is a component of the Cisco Unified Wireless Network.

Cisco WCS provides a full suite of tools for managing and enforcing wireless security configurations and policies within the Cisco wireless network infrastructure. These include:

- Network security policy creation and enforcement, such as user authentication, encryption, and access control
- Wireless infrastructure security configuration
- Rogue detection, location, and containment
- Wireless intrusion prevention system (WIPS)
- Wireless IPS signature tuning and management
- Management Frame Protection (MFP)
- Collaboration with Cisco wired Network IPS for monitoring and mitigating unauthorized or malicious wireless user activity
- Comprehensive security event management and reporting

In Cisco Unified Wireless Network Version 5.1, a new automated security vulnerability assessment is now available to facilitate analysis of an enterprise's overall wireless security posture, as well as to provide WLAN operators with real-time benchmarking of their security services configurations against industry best practices. The automated security vulnerability assessment provides:

- Proactive vulnerability monitoring of the entire wireless network
- Comprehensive information on security vulnerabilities that could lead to loss of data, network intrusion, or malicious attack

- Reduction in the time and expertise required to analyze and remedy weaknesses in wireless security posture

Features

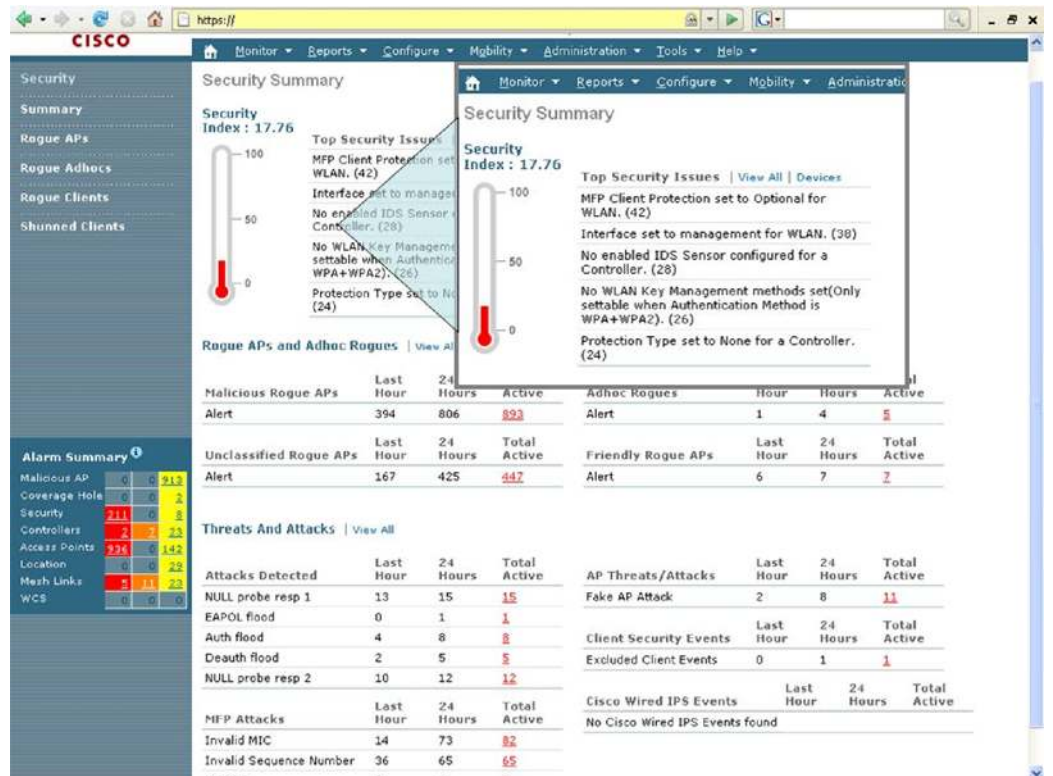
The new automated wireless vulnerability assessment audits the security posture of the entire wireless network for vulnerabilities. These vulnerabilities can result in:

- Unauthorized management access or using management protocols to compromise or adversely impact the network
- Unauthorized network access, data leakage, man-in-the-middle, or replay attacks
- Compromise or adverse impacts to the network through manipulation of network protocols and services, for example through denial-of-service (DoS) attacks

The Cisco WCS automatically scans the entire network and compares settings against Cisco recommended and industry best practices for wireless security configurations. The automated wireless security assessment function within WCS scans wireless LAN controllers, access points, and network management interfaces for vulnerabilities in configuration settings, encryption, user authentication, infrastructure authentication network management, and access control.

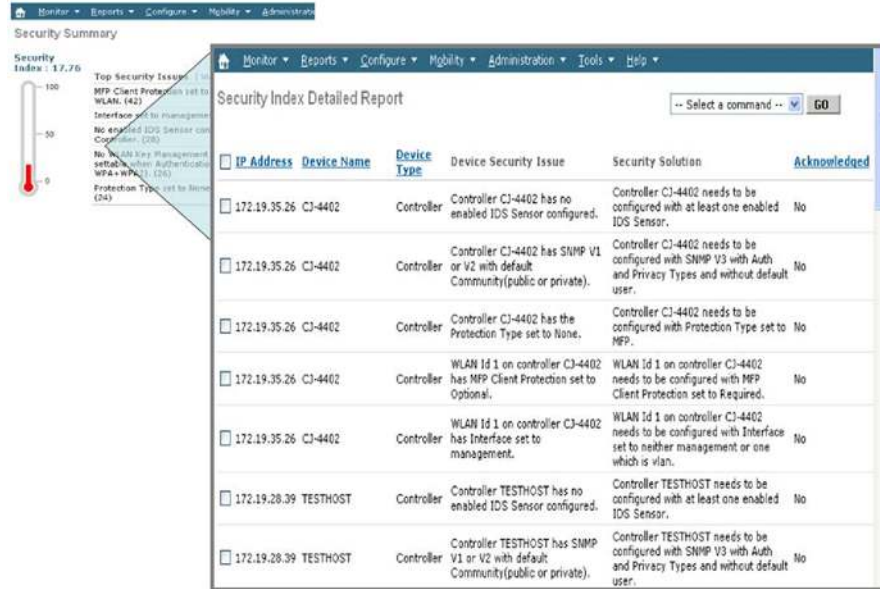
Status of the wireless network security is graphically displayed to provide wireless network administrators with an easy-to-read dashboard of security events. The WCS displays the vulnerability assessment results through a Security Index on the WCS security dashboard. As Figure 1 shows, the Security Index summarizes the network security posture with a composite security score and prioritized summary of vulnerabilities.

Figure 1. Cisco WCS Security Summary



Administrators can drill down to the Security Index Detailed Report (Figure 2) if an event in the Security Summary warrants further investigation. The Security Index Detailed Report provides in-depth analysis of the vulnerabilities across the network. It also identifies optimal security settings and recommends changes that will remedy the vulnerabilities. Any changes the administrator makes are reflected in an updated Security Index score.

Figure 2. Cisco WCS Security Index Detailed Report



Benefits

The single dashboard view of security events within the Cisco WCS provides wireless network administrators with a prioritized report of issues and alarms. This simplified view allows for easier assessment of event severity and enhances the administrator’s ability to quickly prioritize administrative tasks.

Drill-down capabilities allow administrators to investigate and mitigate many issues from a central console, thereby reducing the need for onsite troubleshooting and support. Cisco’s recommended security configurations provide insight and increase administrator confidence when deploying wireless networks.

By providing a consolidated view of security events and alarms with intelligent issue reporting, the new Cisco WCS automated security vulnerability assessment enables administrators to spend less time diagnosing network problems so that they can proactively manage security configurations.

Summary

The Cisco Wireless Control System provides the most comprehensive centralized management system for the Cisco Unified Wired and Wireless Network with a single platform for delivering new features that benefit both IT administrators and network end users. Integrated wired and wireless network security provides the highest levels of protection against attacks and wireless threats with the lowest total cost of ownership.



Americas Headquarters
 Cisco Systems, Inc.
 San Jose, CA

Asia Pacific Headquarters
 Cisco Systems (USA) Pte. Ltd.
 Singapore

Europe Headquarters
 Cisco Systems International BV
 Amsterdam, The Netherlands

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0804R)