Cisco fortifies enterprise wireless LANs with self- defending network

by Bend_Weekly_News_Sources

Unparalleled Wireless Network Architecture Helps Address Stringent Regulatory Requirements for Network Security

Cisco today unveiled a tested and validated wireless solution to secure business critical applications and data, as well as business environments with today's launch of the Cisco Secure Wireless Solution. This solution forges robust network security using Cisco's Self-Defending Network with the latest wireless security features enabled in its Unified Wireless Network.

Ideal for organizations that must meet stringent government regulations, such as Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), and retail's Payment Card Industry (PCI) standard, the Cisco Secure Wireless Solution signals a significant milestone in Cisco's strategy to deliver integrated, advanced technology solutions to address critical business issues.

The Cisco Secure Wireless Solution is an architectural design that builds on the Self Defending Network framework that encompasses a Cisco Unified Wireless Network combined with Cisco's award-winning NAC Appliance, ASA firewall, Cisco Security Agent, Cisco IPS Software, Cisco Secure ACS and Cisco Secure Services Client. The culmination of this fully-tested and validated solution provides IT administrators with a comprehensive set of advanced security features for their wireless LANs, which until now were previously reserved solely for wired-based networks.

"Truly integrated wired and wireless network security is a No. 1 requirement for our customers as they move toward pervasive wireless networks," said Brett Galloway, vice president and general manager of Cisco's Wireless Networking Business Unit. "Today's Secure Wireless Solution takes that fear factor away by mitigating network threats and allowing a business to realize wireless-enabled mobility benefits without compromising regulatory compliance."

Cisco's new Secure Wireless Solution supports the following applications:

Â· Unified wired and wireless intrusion detection (IDS) and intrusion prevention systems (IPS) by way of inspecting traffic flow for harmful applications and blocking malicious client access at the physical layer before network connection can occur;

Comprehensive client validation, posture assessment and remediation for wireless users, which helps ensure wireless clients are up to date with the latest security policies and which mitigates the spread of viruses from uncontrolled wireless networks;

Single sign-on capabilities and 802.1X integration that provides for integrated encryption of wireless client applications and streamlined password management control;

Integrated firewall services for guest access, which helps business provide non-employees and contractors with access to the Internet, while protecting the company's network;

Host intrusion prevention, which prevents wireless clients from being exploited as a bridge into the network and helps protect clients from suspect content and potential hackers;

Rogue detection and containment to proactively help eliminate potential wireless threats from ad hoc client associations and rogue access points.

"With the Cisco Unified Wireless Solution, we have built a best of breed security architecture," said Erik Parker, certified information systems security professional and senior wireless infrastructure analyst of Toyota Motor Sales, U.S.A., Inc. "The security features are an included functionality in our Cisco powered enterprise class wireless network and greatly reduce the total cost of ownership for maintaining a secure wireless LAN."

Business and Security Compliance Provided by Cisco Secure Wireless Solution

Protecting sensitive business and customer data is the driving force behind the latest regulatory requirements of Sarbanes-Oxley, HIPAA and PCI. For publicly traded companies, Sarbanes-Oxley requires that companies maintain internal control structures and procedures, and HIPAA requires safeguards to ensure integrity and maintained confidentiality of patient information. With the Cisco Secure Wireless Solution, companies and healthcare providers can deploy pervasive wireless, knowing that they are meeting these requirements.

Likewise, for retailers, the PCI standard requires that any merchant that uses payment cards must build and maintain a secure network, protect and encrypt cardholder data, and regularly monitor and test its network. PCI compliance is accomplished with the Cisco Self-Defending Network, providing retailers a superior end-to-end wired and wireless solution.

Cisco fortifies enterprise wireless LANs with self- defending network by Bend_Weekly_News_Sources