

Healthcare Insurance Provider Helps Ensure Wireless Security

EXECUTIVE SUMMARY
<p>PACIFICSOURCE HEALTH PLANS</p> <ul style="list-style-type: none"> • Insurance • Springfield, Oregon • 324 employees <p>BUSINESS CHALLENGE</p> <ul style="list-style-type: none"> • Provide pervasive wireless access to company employees • Provide secure wireless Web access to guests and limited intranet access for vendors • Facilitate a single central point of management—to provide a consistent user experience anywhere in the company and to reduce network administration costs • Comply with regulations specific to the healthcare environment
<p>NETWORK SOLUTION</p> <ul style="list-style-type: none"> • Wireless LAN controllers, management software, and access points deployed at headquarters • Wireless LAN controller blades on routers and access points deployed at remote offices
<p>BUSINESS RESULTS</p> <ul style="list-style-type: none"> • Enabled immediate network connectivity for those employees who travel between offices • Increased productivity during conference room meetings • Met the Web connectivity expectations of guests

PacificSource Health Plans Deploys a Cisco Unified Wireless Network to Headquarters and Remote Offices

Business Challenge

Founded in 1933, PacificSource provides medical and dental benefits to more than 4,000 Oregon employers and covers more than 151,000 people with its group and individual health insurance plans. It also provides self-funded employee benefit plans, flexible spending accounts, health reimbursement arrangements (HRAs), and COBRA administration services through its subsidiaries, Manley Services and Select Benefit Administrators.

The company has long maintained a sophisticated suite of software applications to manage its business. In 2006, PacificSource launched a major software project—upgrading and converting its main insurance claims processing system. The IT team realized that the project would require outside contractors to visit the company’s main campus for several days at a time. “We knew that we were

going to have a number of consultants and third-party vendors on site,” says Erick Doolen, CIO of PacificSource. “And we wanted to be able to provide them with network access.”

The team also wanted to make it easier for PacificSource employees to gain network access when traveling to any of the company’s five satellite offices. At that time, such employees would have to find an Ethernet connection and authenticate themselves. “With our old model, employees who traveled to remote offices would have a cheat sheet that told them how to manually configure the network settings,” says Tim Wolfe, network security administrator at PacificSource—noting that this posed major security risks because it is easy to lose a piece of paper.

Finally, PacificSource wanted to offer Web access to potential customers and other visitors.

Doolen and Wolfe knew that a wireless LAN deployment would be the most sensible way to meet these three new network needs. But the team needed to make sure that such a deployment would meet the strict federal security standards that apply to any company that keeps confidential member data on its network.

“All of our IT decisions are regulated by the general guidelines for HIPAA (the Health Insurance Portability and Accountability Act of 1996),” Doolen says.

Network Solution

PacificSource decided to deploy the Cisco® Unified Wireless Network, made up of access points that could associate with WLAN controllers for advanced features and be managed and configured from a central point, the Cisco Wireless Control System (WCS). Cisco was already the trusted provider of the company's Ethernet switches and routers. After a brief evaluation, the team found that the features of a Cisco centralized WLAN would meet the company's security needs while offering ease of management.

"This centrally managed architecture has a lot of benefits," Wolfe says. "There is less administration required than under older wireless LAN models, because the configuration is all central and automated."

At the company's headquarters in Springfield, the IT team installed 12 Cisco Aironet® 1100 Series wireless access points and two Cisco 4400 Series Wireless LAN controllers, one to control the access points and the other to provide redundancy. In addition, the team adopted WCS management software. Cisco WCS includes graphical tools for wireless LAN planning and design, configuration, RF management, intrusion prevention, and location tracking of clients on the network. With WCS, network administrators can detect both rogue access points and unauthorized clients that attempt to connect to the network. In addition, "The WCS central management allows us to manage the infrastructure at this site and at the remote sites from a single application," Wolfe says.

At each of its remote locations, the PacificSource IT team installed one or two 1130 Series access points, along with a Cisco 2800 Integrated Service Router that was equipped with a Wireless LAN Services Module that plays the same role as the WLAN controllers in the headquarter. The team had wanted to upgrade the Ethernet routers in these locations anyway, and the ISR provided secure routing along with wireless capabilities. Providing multiple functions with a single product resulted in cost savings for the company, and it saved space as well—the ISR is only one U (1.75 inches) high, so it requires very little room in a networking closet.

"PacificSource saw an opportunity to extend the wireless services to the remote sites and take advantage of the integrated network of the ISR platform," says Ethan Meyer, account manager at Cisco.

"The Cisco Wireless Control System (WCS) central management allows us to manage the infrastructure at this site and at the remote sites from a single application."

— Tim Wolfe, network security administrator, PacificSource

The scalability of a Cisco Unified Wireless Network allows for the creation of multiple virtual networks within a single WLAN, and PacificSource took full advantage of this feature. Back at headquarters, the team set up three separate Service Set Identifiers (SSIDs), one for each user group that needed wireless network access. Employees received complete corporate network access, visiting vendors received access to the Web along with limited data in the corporate network, and guests received basic external Web access. The guest network was set up to connect directly to a firewall. The vendor network was connected to a DMZ (demilitarized zone)

port. “If a vendor needs to get to a particular internal server, we can customize it on a per-need basis,” Doolen says.

The team also set up a fourth SSID for testing purposes; the team will add more virtual networks as new applications require.

Business Results

Because of its ability to integrate with the existing Cisco wired network, the wireless LAN deployment went very smoothly. The PacificSource IT staff says the addition of a wireless network proved valuable to the vendors and contractors involved in the claims processing systems upgrade. Because they had immediate access to the network, they spent all their time productively instead of having to search for a network connection. This yielded significant savings in hourly contractor billing.

Since then, employees have continued to use the wireless network at headquarters. “We are noticing more and more people taking their laptops with them to meetings in our conference rooms,” Doolen says. “We have a lot more employees spending time in meetings together than before we installed the wireless network. The ability to collaborate while connected to the network lets them use those meetings more productively.” The fact that employees can share online presentations instead of distributing printouts is saving on paper costs, he adds.

Wireless access has also proven invaluable to mobile employees. “When people travel between offices, we do not have to do anything to get them connected to the network; they can just get right to work,” Doolen says. “That is a big productivity boost for both the IT staff and the sales people who travel frequently.”

PRODUCT LIST

- Cisco Aironet 1100 Series Access Points
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 2800 Series Integrated Services Routers
- Cisco Wireless LAN Controller Modules
- Cisco Wireless Control System Software

Automatic authentication for these traveling employees also helps ensure that network information does not fall into the wrong hands.

“Instead of carrying around a cheat sheet for manual configuration—which they could easily lose—once they are set up on an authorized machine, they can always get network access,” Wolfe says.

Finally, wireless access provides a positive experience for guests. “We are at the point now that people expect wireless,” Doolen says.

NEXT STEPS

PacificSource is deploying a voice over IP implementation later in 2007, with plans to deploy wireless VoIP handsets in the next few years. Wireless VoIP requires a high quality of service, and the IT team is confident that the network will be ready to handle it. “A big reason that we like the centralized management architecture is that it lets us achieve a necessary level of QoS (quality of service,)” Wolfe says.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 528-4000
800 653-1715 (toll free)
Fax: 408 527-0629

Asia Pacific Headquarters
Cisco Systems, Inc.
16B Robinson Road
#29-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7798

Europe Headquarters
Cisco Systems International BV
Hoeiendorpweg 13-19
1101 CH Amsterdam
The Netherlands
www.europe.cisco.com
Tel: +31 20 620 6781
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. CDM, the Cisco logo and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work™, Live, Play, and Learn is also a Cisco mark of Cisco Systems, Inc., and Apposa, Register, Attend, EPK, Catalyst, CDDA, DCDP, DCE, CDR, CDNA, CCNT, CCEP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, EtherFast/Ether, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GetAnywhere, HomeLink, Internet Quicker, IOS, Phone, IPTV, QoS Certified, the QoS logo, QoS Ready, QuickStart, CiscoStream, Linksys, Meeting Place, NCC, Networking Academy, Network Registrar, Packet, PIX, PreConfig, RateMUX, SanJose, SecureCast, SVA/AVI, BlackWire, The Better Way to Increase Your Internet Quota, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in the 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. (C/01.0)