Cisco Workforce Connects to a Borderless Network from Any Device

BUSINESS BENEFITS

- Increased productivity and employee satisfaction
- Enabled self-provisioning
- Saved US$500,000 annually in helpdesk costs
- Strengthened end-to-end security

"At Cisco, the question is not if we'll become a true borderless enterprise, but when. One step on the journey is enabling our mobile workforce to use any device to securely connect to the Cisco enterprise network, a goal we've achieved with AnyConnect."

Rami Mazid, Vice President of Client Services, Cisco IT

AnyConnect client provides secure remote access from laptops, tablets, and handhelds

Cisco wants to give employees the flexibility to work from anywhere, using any device—a borderless experience. But with the previous VPN client, employees had to manually reconnect and reauthenticate whenever they moved out of the coverage area.

In addition, helpdesk costs associated with one-time passwords for the VPN client approached $500,000 annually. More costs arose from having to support different VPN clients for each type of devices Cisco employees use for work. These include Symbian OS-based Nokia dual-mode phones, Windows Mobile Operating System devices, Apple iPhones, Android phones, Apple iPads, Cisco Cius tablets, and Windows, Mac, and Linux desktops and laptops.

Now Cisco uses the AnyConnect Secure Mobility Client. The same software works on all devices used within the company, and Cisco IT is beginning with Windows and Mac devices. After self-provisioning the client, Cisco employees can connect to the Cisco network from any location with an Internet connection, just as they would in the office.

Employees can be more productive because Cisco AnyConnect is always on. They no longer need to re-enter a one-time password to reestablish a dropped connection**.**

Centralized management saves time for Cisco IT throughout the client software lifecycle. Employees self-provision from the service catalogue web page, without IT involvement. In addition, Cisco IT no longer needs to spend time troubleshooting when employees experience problems with the VPN access software. Instead, employees simply visit the provisioning website to download the software again.

Security is strong, because AnyConnect provides both authentication and PKI-based device authorization. This is fully automated, a significant timesavings in a 70,000-person organization. To make sure a device attempting to establish an SSL VPN session is registered, the solution checks the device's certificate against its serial number. Requiring device registration also associates the device with a person, aiding security investigations and helping to ensure end-user accountability.

Cisco AnyConnect also mitigates the risk when employees lose their devices. When an employee informs Cisco IT of the loss, Cisco IT can immediately terminate any active VPN sessions for the asset on the headend and prevent any further VPN connections. Cisco IT can also easily terminate accounts of employees who leave the company.

FOR MORE INFORMATION

To read the entire case study or additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

All contents are Copyright © 2011 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

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 Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; 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, MeetingPlace Chime Sound, 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. (0807R)

(C) 2008 Cisco Systems, Inc. All rights reserved.