

How Cisco IT Provides Remote Access for Small Offices and Telecommuters

Enterprise Class Teleworker Solution improves reliability, availability, and security for small- and home-office users.

Cisco IT Case Study / Security and VPN / VPN Remote Access Solution: Cisco Enterprise Class Teleworker (ECT) solution is an integral part of the Cisco Service Oriented Network Architecture (SONA) framework, guiding customers to achieve Intelligent Information Network (IIN) in their Enterprises. This case study describes the deployment of ECT within Cisco's own network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

“Time-zone challenges are a common theme for global companies like Cisco. The Enterprise-Class Teleworker solution enables early morning conferences calls with EMEA and late evening calls to India and AsiaPac, without having to be in the office. My productivity and efficiency have increased considerably, with a functional work environment at home.”

– **Bob Scarbrough, Senior Project Manager, Information Technology (Cisco on Cisco)**

BACKGROUND

More and more companies are discovering the benefits of teleworking, which extends a company's network infrastructure to remote and home-based workforces, improving productivity, satisfaction, and retention. At Cisco Systems®, high-speed remote access means employees can perform almost all their work-related functions from home. For many employees, this translates to an additional 10 to 40 percent productivity per day. In fact, some work can be done more efficiently from home, where interruptions or phone calls are less likely. Cisco® employees also find that high-speed remote access makes it easier to balance their work and home lives, which improves morale and makes it easier to retain valuable employees. In addition, reliable high-speed remote access has enabled employees that have moved away from Cisco locations to remain with the company.

Remote access helps employees support globalization and collaboration worldwide. With Cisco's global presence, employees regularly need to collaborate across continents and time zones. Remote home access eases the burden of attending meetings outside of regular business hours. Remote access also provides the flexibility for employees to continue working from home in an emergency, such as severe weather, outbreak or a disaster that prevents them from coming into the office. This greater worker flexibility provides an extra layer of resilience in keeping Cisco running under adverse conditions.

In 2002, approximately 37 percent of the U.S. working population was classified as teleworkers—either part-time or full-time teleworkers or day extenders (employees who telecommute evenings or weekends to stretch their workdays). Market intelligence firm IDC estimates that this figure will double to 50 million by 2006. At any given time, out of Cisco's 50,000 users, there are about 10,000 remote-access sessions in use, including employees and contractors. Among the categories of teleworkers at Cisco:

- Full-time teleworkers who work from a fixed external site, usually their home
- Part-time teleworkers who telecommute a few days a week

- Part-time employees who work from home
- Day extenders who telecommute evenings or weekends
- Part-time teleworkers, including consultants, who telecommute because of specific projects

In 2001, to deliver home-based remote access to its users, Cisco IT introduced a software-based virtual private network (VPN) solution. This solution provided the necessary security and authentication features that Cisco IT demanded, but establishing a connection took time and lacked some important features. Once the VPN client was loaded onto their PC, users would connect to the Internet, connect to a headend VPN concentrator at the Cisco corporate VPN hub site, log on and authenticate and, finally, establish a secure, one-to-one connection with the corporate network. This software-based VPN worked well for Cisco employees who needed to connect their laptop to the corporate network over the Internet from home. It worked equally well for employees who needed to work from hotel rooms, airports, coffee shops, or other locations where Internet access (wired or wireless) was available.

For most teleworkers, this was adequate. But for those who required more sophisticated connectivity at home, the software VPN solution had limitations. Teleworkers could not connect more than one device to the network. The VPN client only supported the device it was installed on. Other devices, such as additional PCs, print servers, or printers, were not recognized by the network. Many Cisco employees wanted to connect several devices to the corporate network, but with the VPN that was in place, were unable to do so.

Another major limitation was the lack of support for IP phones—a critical item for home offices. There was no jack on a PC or laptop to “plug” these phones into. Cisco IP Communicator, a software-based IP phone, partially resolved this issue, but the lack of quality of service (QoS)-based traffic prioritization made IP voice calls vulnerable to quality issues. When an IP phone user sent large file packets over their limited remote-access Internet link while talking on their IP phone, voice quality would often suffer. Voice packets would be delayed or dropped behind the large file packets, causing the voice call to have silent gaps or crackling static sounds.

The Cisco Security Technology Group reasoned that a hardware-based VPN model could better meet the demanding needs of a full home-office environment, and set out to create a next-generation solution. The solution centered on Cisco IOS® Software, which supported VPN IP Security (IPSec) standards as well as the security and QoS features on Cisco routers. In addition, Cisco IOS Software supported a new architecture called Dynamic Multipoint VPN (DMVPN). DMVPN transforms the Internet into a virtual “office network,” enabling high-performance networking to remote-access users across the Internet without the users having to connect through Cisco corporate VPN concentrators. Using DMVPN, for example, a Cisco employee in South America could work with another Cisco employee in Florida, using IP telephony, IP video, or other peer-to-peer collaborative applications, and connect across the shortest Internet path, rather than being connected through the nearest Cisco network hub location (in this case, Research Triangle Park [RTP], North Carolina). Similarly, two users in Canada could bypass the Cisco hub in Boston, and two users in Denver could communicate without connecting through San Jose, California.

Rather than relying on a software VPN client within a teleworker’s PC, the new teleworking solution would use a dedicated Cisco router at the remote user end that was “always on.” The router would have multiple ports to support multiple devices, independent of the device operating system. And the router would also provide multilayer security based on Cisco IOS Software.

CHALLENGE

To assist in developing and testing the new solution, the Cisco Security Technology Group and Cisco IT initiated and managed an internal trial in late 2002. By March 2003, more than 500 Cisco teleworkers were participating in the trial. While the business unit’s ongoing development efforts focused on end-to-end connectivity, QoS, and end-to-end security, Cisco IT recognized some practical issues related to provisioning and managing a large-scale solution that needed to be addressed.

While many of the early trial users had engineering or technical backgrounds, this would not be true of the wider

range of users the service would eventually be deployed to—these teleworkers would require a greater level of Cisco IT support. Technically proficient teleworkers, however, might attempt to customize their router configurations, which could complicate network management, leading to an increase in support costs and reduction in the level of service. Remotely supporting many types of routers could also complicate management efforts. Nonstandard hardware or configurations would make it difficult for IT to automate the process of providing updates and software upgrades, which is critical if an update is needed to patch an immediate security vulnerability. And manually managing and updating each of the thousands of routers would increase the IT cost burden on the corporation, reducing its ability to compete. Because of this, Cisco IT usually provides services to the entire corporation when management and maintenance can be automated.

During the initial trial, each Cisco router was manually configured by a Cisco IT technician before being sent to the teleworker. The engineer followed a lengthy process to generate a configuration, and then manually copied the configuration onto the new router. The challenge of provisioning so many new routers concerned Cisco IT. A survey of the industry identified several common deployment scenarios: 1) Manually configure each router internally and ship it to the user; 2) Ship routers to a staging facility operated by an ISP, where the routers are configured and then shipped to the user; or 3) Contract with a company to configure and install routers. Each of these scenarios added between US\$70 and \$120 to the cost of deployment. “Our best engineer working as quickly as possible would configure a router in about 45 minutes,” says David Iacobacci, network engineer for Cisco IT. “Using this method, it was impossible for Cisco—or any company—to add hundreds or thousands of teleworkers.”

In addition to configuration challenges, the prospect of remotely managing thousands of routers located in employees’ homes was a significant concern for Cisco IT. The labor-intensive provisioning process and the network management of so many devices had to be addressed.

SOLUTION

In March 2004, Cisco IT agreed to assume support responsibility for most of the 500 pilot users and take the lead role in developing provisioning and management processes. Cisco IT’s goals included:

- A secure VPN remote-access service
- A global deployment and support model
- Global management capabilities
- Low total cost of ownership

This new teleworking solution would be built on the four main constructs of the Cisco Enterprise-Class Teleworker solution: end-to-end connectivity, deployment, management, and security—end to end not just in the physical sense, but throughout the entire lifecycle.

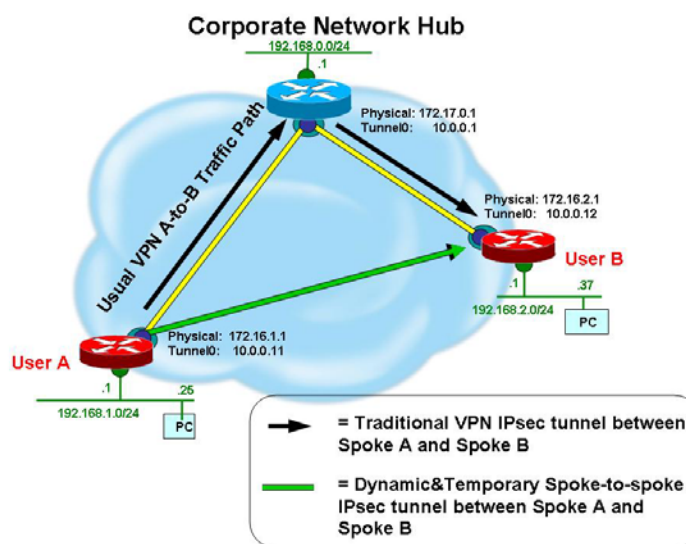
VPN Service Features

The Cisco Enterprise-Class Teleworker solution combines a router—in early 2006, the Cisco 800 Series router—with a high-speed broadband connection (DSL or cable) at the Cisco employee’s home. This Cisco IOS Software-based router provides hardware-based IPsec, Triple Data Encryption Standard (3DES) encryption, and an enhanced set of security features. The features include stateful inspection firewall capabilities; public key infrastructure (PKI) and authentication, authorization, and accounting (AAA) security integration; IPsec Network Address Translation transparency (NAT-T); and user and router authentication using authentication proxy (auth-proxy) at the router and Cisco Access Control Server (ACS) in the hub. With the Cisco IP Solution Center (IPC) appliance, security policies and Cisco IOS Software version updates can be automatically pushed to the router, ensuring that the home user has the latest and most secure software. The hardware VPN service also provides QoS for future voice and potential video services support, and remote management capabilities that allow Cisco IT to monitor, configure, and upgrade the routers from a central location. The Cisco Enterprise-Class Teleworker solution provides a secure, encrypted,

always-on connection that is easy for the user to set up and use, and easy for Cisco IT to manage.

The central technology behind the Cisco Enterprise-Class Teleworker solution is DMVPN, which provides secure, end-to-end VPN connectivity over the Internet to support multiple, best-path tunnels between and among multiple users. Traditional remote-access solutions require multiple remote users to set up tunnels from their locations to a central remote-access hub concentrator and communicate with each other through the hub. DMVPN, on the other hand, allows remote users to locate each other through the hub and establish secure, encrypted tunnels directly to each other through the Internet, bypassing the remote-access hub (Figure 1). This is a far more scalable way of building secure, collaborative, peer-to-peer connections over the public Internet.

Figure 1. DMVPN Tunneling



Cisco IT could not meet demand for new users when a technician could, at best, preconfigure six to eight routers per day. To make the Cisco Enterprise-Class Teleworker solution globally scalable, a new type of provisioning was needed. “Zero-touch” provisioning automates the configuration process, eliminating virtually all the time and effort previously spent by technicians and simplifying the installation process for the user. From the user’s perspective, the entire provisioning process takes just three to four minutes.

Zero-Touch Provisioning Process

Zero-touch deployment can be described from the user’s perspective as well as from the back-end process perspective.

From the user’s view:

Step 1: The user submits a request for new service, which includes specific ISP-related information

Step 2: The user receives the new router at home

Step 3: The user connects the router to the existing ISP equipment and obtains ISP connectivity

Step 4: The user types a URL into the browser address field (this URL is sent to the user upon manager approval)

Step 5: When prompted, the user types in his or her user name and password

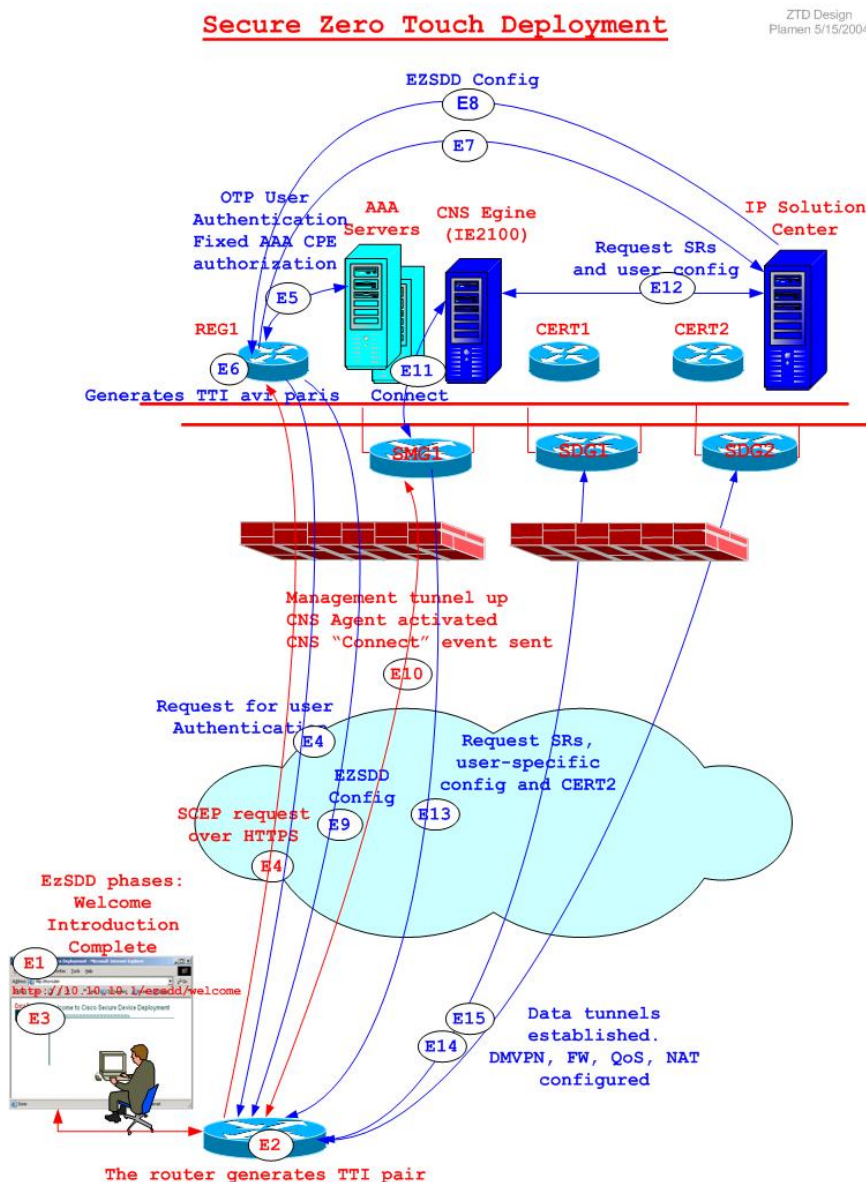
Step 6: Within four minutes, the user is notified that the process has been completed

The back-end process is as follows:

Step 1: Upon approval by the manager, the Cisco 800 Series router configuration is automatically processed by the Cisco IP Solution Center. The Cisco IP Solution Center belongs to a family of intelligent management applications that help reduce overall administration and management costs by providing automated resource management and rapid profile-based provisioning capabilities that enable fast deployment and time to market. The Cisco IP Solution Center has traditionally been used in service provider and large enterprise networks.

Step 2: When the user plugs in the new router, the router “calls home” to the Cisco IP Solution Center. At that point, the Cisco IP Solution Center pushes policies to the router, including changing the IP addresses or IP subnet of the user, assigning a predefined IP address space for the user, applying IPSec policies, applying firewall and user authentication policies, applying QoS policies, and applying NAT. “This ability to push policies to remote routers was new for Cisco,” says Plamen Nedeltchev, architect of the Cisco IT deployment. Once this process is complete, the user logs in, enters a password, and is connected to the Cisco corporate network.

Figure 2. Enterprise-Class Teleworker Solution Provisioning Process



Management Process

Several components combine to provide management of the Cisco Enterprise-Class Teleworker solution. These include Cisco's internally developed enterprise management tool (EMAN), the Cisco IP Solution Center (ISC), and the Cisco CNS 2100 Series Intelligence Engine. EMAN performs resource monitoring, automatic page alerting, change management tracking, and availability measurements across the worldwide Cisco network. When a new user request is approved, EMAN assigns a subnet for the home network, creates a login account with the Cisco Secure ACS server, and passes that information on to the Cisco IP Solution Center.

The Cisco IP Solution Center software application runs on a UNIX server that manages various types of connections between central servers and remote clients. It is used specifically within the Cisco Enterprise-Class Teleworker solution to generate and maintain router configurations and policies. The Cisco IP Solution Center does not communicate directly with the Cisco 800 Series router. Instead, configurations and policies created by the Cisco IP Solution Center are forwarded to the Cisco CNS 2100 Series Intelligence Engine (also known as the configuration engine).

The Cisco CNS 2100 Series Intelligence Engine runs on a Linux server and downloads the configuration and policy information to the remote Cisco 800 Series router. It communicates with the router through a management tunnel, which is separate from the two data tunnels.

The Cisco IP Solution Center and CNS 2100 Series Intelligence Engine also play a major role in ongoing management. Through a feature known as fully managed service, whenever a configuration change occurs on a Cisco router, the router will notify the configuration engine of the change. The configuration engine, in turn, notifies the Cisco IP Solution Center, which will confirm that the appropriate policies are still in force on the router. In addition, when changes are made to the standard policy, the Cisco IP Solution Center drives changes through the configuration engine to the routers. Also, ongoing events that occur on the Cisco routers are logged by the configuration engine, copied to EMAN, and can be accessed through a Web interface. Approximately two weeks of events can be viewed. Finally, the configuration engine can be used to perform Cisco IOS Software image management on the routers.

In August 2004, the Cisco Enterprise-Class Teleworker pilot test was declared a success and became a full-production service.

RESULTS

Through the Enterprise-Class Teleworker solution, Cisco has created a sustainable global deployment and support model capable of meeting the needs of teleworkers around the world. It provides global management capabilities that ensure reliability, availability, and security. "The Enterprise-Class Teleworker solution combined different Cisco technologies," says Nedeltchev. "Integrating those technologies and capabilities into a single device while maintaining low TCO was the biggest challenge of this project. But it was a challenge we met through zero-touch deployment."

Zero-touch deployment was nominated for the Cisco's internal Outstanding Core Technology Award for 2005 for its contribution to lowering costs. Typically, deployment and support of a service represents a large portion of the total cost of ownership. Zero-touch deployment is expected to reduce this cost by 20 percent or more.

DMVPN and the Cisco Enterprise-Class Teleworker solution were awarded the Cisco Pioneer Award in 2004 because of the extensive list of innovative features that were built into the solution. "We challenged some of the expectations of the way Cisco IT does business in the name of innovation," says Nedeltchev. "The Enterprise-Class Teleworker solution has many components, and innovation was the driver."

Among the "firsts:" the proof of concept of DMVPN; the first use of a PKI infrastructure within the IT environment; the first implementation of zero-touch deployment; the first fully automated end-to-end deployment, provisioning, management; and for the first time, the ability to push changes and apply security policies in real time without

disrupting the end user's connection.

Based on its success in the Cisco Enterprise Class Teleworker solution, zero-touch deployment will be expanded into other areas of Cisco products and solutions.

The User Experience

Teleworkers have gained significant benefits with the Cisco Enterprise-Class Teleworker solution, compared to the previous software VPN service. Because the solution is an "always-on" service, users can simply turn on their PC and log in, and they are immediately connected—as if they were in their office. The tedious and time-consuming process of establishing a VPN session is eliminated. Working early or late is made easier, and jobs can be set to run overnight. "There is a significant contrast in how I use my laptop now," says Thomas Herbst, a solution user. "With the Cisco Enterprise Class Teleworker solution, I leave my laptop on most of the time after hours and on weekends. If I think of some small work-related task, an e-mail I forgot to send, or a document reference I forgot to check, I'll just walk to my home office and do it then. Before, it could be two or three minutes before I had a working connection. That may not sound like a long time, but it was long enough that I might put off doing the small tasks until the next time I connected—and hope I recall that other task I was supposed to do."

This aspect of connectivity was addressed in a survey conducted by Cisco IT during the initial trial of the Cisco Enterprise-Class Teleworker solution. According to respondents, 95.3 percent expected the solution to increase their productivity at home. In the same survey, 81.3 percent said that the solution had increased their availability to be online with an average of 6.5 hours per week, and 80 percent said that the solution had also increased their overall working hours. As one user stated, "I have employees in Europe and partners in Asia. The hours and activities that comprise my job do not all mesh easily with the Cisco office environment. The Cisco Enterprise-Class Teleworker solution allows me to work with EMEA before breakfast, without having to get dressed, and with Asia after my family has gone to bed. If I had to be in the office that many hours, I wouldn't do the job. The Cisco Enterprise-Class Teleworker solution allows me to work on the more confidential and sensitive projects without requiring (me to) have a more expensive office at work."

Support for multiple devices is another big benefit for teleworkers that need it. "The main value of the Cisco Enterprise-Class Teleworker solution for me is hooking up my Windows laptop and Linux desktop so they can both access the Cisco network, the engineering labs, and each other," says Stuart Taylor, Cisco engineer. "With the software VPN, I had two machines sitting on my desk that wouldn't talk to each other, which was inconvenient when I needed to copy files between them."

Having the office at home provides a more flexible work environment, which can increase job satisfaction. The Cisco Enterprise-Class Teleworker solution also allows employees to move away from an office location—to another county, another state, or even across country if needed. And it enables employees to even work globally more easily.

Finally, zero-touch provisioning has streamlined and simplified the installation process for new Enterprise-Class Teleworker solution users. One user remarks, "Deployment was easy. I plugged the router in and it worked right away."

The Corporate Experience

Cisco has very conservative security policies, with a consistent posture of low risk taking. The Enterprise Class Teleworker solution minimizes risk through comprehensive, multilayered security features. "You cannot approach security only at the user level or device level," says Nedeltchev. "You must approach it across the system, providing authentication, authorization, and posture, which in turn constitutes a trial of trust." From a support perspective, the solution simplifies the management of the environment and allows comprehensive analyzing and automated decision making.

The Cisco Enterprise-Class Teleworker solution provides layers of security that are incorporated into Cisco IOS

Software and the Cisco dynamic routing protocols framework. Users must have a valid Cisco.com account password to apply for teleworking service. When they set up their router, they must have a one-time password to configure the device. Then, the system requires a user password whenever they log onto the Cisco network. And finally, the router itself must be authenticated by the system when login occurs.

Other security features include the ability to automatically disconnect a terminated employee within seconds and, if password recovery is attempted or the user changes the host name of the router, the remote router will lose its private keys and any attempt to log on will fail.

With the added flexibility and access the Enterprise-Class Teleworker solution provides teleworkers, employees can be more productive. This ability to perform their job more efficiently and effectively leads to greater satisfaction and retention.

Cisco IT Experience

The Cisco Enterprise-Class Teleworker solution offers significant benefits to Cisco IT through its provisioning and management capabilities. Zero-touch deployment reduces Cisco IT involvement to truly zero and significantly increases scalability. The number of new users is no longer limited by the number of routers a technician can preconfigure in a day. Prior to the deployment of the Enterprise-Class Teleworker solution, Cisco managed about 2400 routers in its worldwide network and added perhaps as many as 10 per month. With zero-touch deployment and integrated management, Cisco IT can support another 35,000 routers on its network. Zero-touch deployment, DMVPN, managed multilayer security, policy push, and automated image management allows large-scale deployments, like 50,000 routers, while maintaining low total cost of ownership (TCO).

“Cisco IT has already subscribed more than 4000 employees to the Enterprise-Class Teleworker service, and anticipates that more than 20,000 employees will eventually decide to use the service,” says Nedeltchev.

LESSONS LEARNED

Because of the lack of experience with the zero-touch provisioning capability, Cisco IT proceeded cautiously, limiting the number of users added so as not to overload the system. However, these concerns were unfounded, and the zero-touch feature worked flawlessly.

NEXT STEPS

The Cisco Enterprise-Class Teleworker solution is being introduced incrementally. DMVPN is currently implemented in a hub-to-spoke configuration; spoke-to-spoke or end-to-end DMVPN IP will be introduced next. This will allow teleworkers to establish secure IP tunnels directly between or among their home offices instead of connecting through the corporate hub site.

Security

Cisco has evolved a security strategy for the Enterprise-Class Teleworker solution in three primary phases.

Phase 1 achieved an integrated security solution, where every network element is a point of defense, including routers, switches, appliances, and endpoints.

Phase 2, in process, involves creating a collaborative security system where security becomes a collaborative network wide system between the endpoints, network, and policies in an active management solution. A core element of collaborative network security is Cisco Network Admission Control (NAC), deployed to enforce a corporate security policy of requirements for any client device on the network. Cisco NAC seeks to ensure the health of all client workstations prior to those workstations being granted network access. As a technology, NAC works in conjunction with many workstation protection software packages, including system patches, Cisco Security Agent, and third-party antivirus software to assess the condition or “posture” of a client prior to granting network access. This ensures a

workstation has, for example, an up-to-date system patch, software hot fix, Cisco Security Agent version, and virus signature set—and has not been infected prior to gaining access to a data network. If the workstation requires a software package update, an action is sent back to the workstation directing it to complete the update. If the workstation has been compromised or a network outbreak has occurred, the workstation is placed into a quarantined network segment where it can get the upgrades and patches necessary to conform to the corporate security policy.

Phase 3 will establish an adaptive threat-defense system, where security services and network intelligence work together proactively to improve operations efficiency and optimize protection all the way up to the application level. Cisco network and security elements will work together to control access; inspect packets; provide application intelligence, content inspection, and virus mitigation; and manage identities and traffic visibility. Collectively, this provides application security and defense, containment, and control mechanisms to secure the entire network and all services. Cisco refers to this adaptive threat-defense system as a Self-Defending Network.

Media Support

The Cisco Enterprise-Class Teleworker solution already supports cable and DSL. Other mediums to be supported in the future include VPN over satellite and VPN over wireless WAN. VPN over satellite will offer connectivity to users in areas where no cable or DSL is available. There are currently several dozen solution users piloting this service.

VPN over wireless WAN services are already being planned. Several cities have initiated services that support high-speed connectivity over 802.11b. Companies are also developing 2-Mbps service for dual access to Global System for Mobile Communications (GSM) or Code Division Multiple Access (CDMA) phones, and Intel is currently working on 100-Mbps wireless WAN technology. Cisco IT will evaluate these new technologies for eventual support within the Enterprise-Class Teleworker solution.

Integrated Services

The Cisco Enterprise-Class Teleworker solution currently supports secure, fully managed data services. However, if a user wishes to have IP telephony through their Cisco 800 Series router, they must request voice service separately. A future phase of the Cisco Enterprise-Class Teleworker solution will bundle both encrypted data and encrypted voice in a single service bundle. Wireless LAN will also be incorporated, allowing teleworkers to use their laptop from anywhere in their house. Video is also being considered for the Enterprise-Class Teleworker service bundle.

Beyond Home Use

The Cisco Enterprise-Class Teleworker solution has been positioned and deployed as a home-office-based service for teleworkers. However, the same technology can be applied to connecting small offices currently supported over a WAN, and Cisco partner locations supported over VPN extranets. With the introduction of more powerful routers, even larger sites could be served where it makes business sense.

Management Hubs

Cisco IT supports 4 management/data hubs in San Jose, RTP, Amsterdam, and Hong Kong. Besides, Cisco IT supports 6 Data Hubs in Richardson, Texas; Boxborough, Massachusetts; Natania, Israel; Tokyo, Japan; Hong Kong; Singapore and Sydney, Australia. As budget and resources permit, Cisco IT will expand to India and other locations as well.

Management hub sites currently use Cisco 7200 Series routers, which support up to 750 users. The recent advancements in DMVPN will allow Cisco IT to terminate and support up to 2000 devices per Cisco 7200 Series router. Cisco IT is evaluating Cisco Catalyst® 6500 Series switches, which can support up to 5000 users each.

Additional Information on the Cisco Enterprise-Class Teleworker Solution

- Cisco Enterprise-Class Teleworker solution: www.cisco.com/go/ect
- Packet magazine article on DMVPN and Business Ready Teleworker:

<http://www.nxtbook.com/nxtbooks/cisco/packet-2q-04/index.php>

- Packet magazine article on Business Ready Teleworker (Second Quarter, 2004 issue, p. 13):
<http://www.cisco.com/web/about/ac123/ac114/downloads/packet/packet/apr04/pdfs/apr04.pdf>.

FOR MORE INFORMATION

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

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.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 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. CCVP, 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 a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, 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 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. (0705R)