How Cisco IT Provides Remote Network Access for Small Offices and Teleworkers

The Cisco Virtual Office solution improves the reliability, availability, and security of Cisco's VPN.

Cisco IT Case Study/Security and VPN/Cisco Virtual Office Solution: The Cisco® Virtual Office solution extends the Cisco routed intranet, via secure VPN Internet connections, into thousands of employees' homes and, in the future, small offices. This case study describes the deployment of the Cisco Virtual Office solution within Cisco's own network, an advanced enterprise environment that is one of the largest and most complex in the world. As of mid-2008, Cisco had more than 15,000 internal users for the Cisco Virtual Office solution. This deployment is yielding the benefits of increased employee productivity and job satisfaction, IT cost savings, and reductions in Cisco's environmental impact. Customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

BACKGROUND

More companies are discovering the benefits of teleworking, which extends a company's network infrastructure to remote and home-based employees while improving their productivity, satisfaction, and retention. A few statistics show how this work model is becoming important to many types of organizations:

> "My productivity and efficiency have increased considerably with a functional work environment at home."
>
> **Bob Scarbrough, IT Manager, Cisco IT**

- An IDC forecast from December 2007 "expects the global mobile worker population to increase from 758.6 million in 2006 to more than 1.0 billion in 2011, representing just over 30 percent of the worldwide workforce."
- Teleworkers create a significant cost savings. For example, each full-time teleworker means US$22,000 in reduced costs per year for commercial real estate.
- The environment also benefits from remote work, with reductions in carbon dioxide emissions and US$500 gasoline cost savings annually for each employee who works one day per week from home.

At Cisco, high-speed remote network access means employees can perform almost all work-related functions from home. In fact, some work can be done more efficiently from home, where interruptions or phone calls are less frequent.. Time saved by not driving to the office is often used by employees to perform productive work. Energy savings are also achieved by employees who avoid the traditional commute to work.

Cisco employees find that remote access to the Cisco network makes it easier to balance their work and home lives, which improves morale and makes it easier for Cisco to keep valuable employees. In addition, reliable VPN access has enabled employees who have moved away from Cisco locations to remain with the company.

EXECUTIVE SUMMARY

BACKGROUND

- The Cisco VPN provides remote access to the corporate network for thousands of employees and other authorized users

CHALLENGE

- Provide network access features that cannot be supported on a software VPN client
- Automate and simplify router provisioning and updates
- Enable a scalable VPN solution to support up to 30,000 users

SOLUTION

- Cisco Virtual Office solution with Cisco 800 Series Integrated Services Routers
- Dynamic Multipoint VPN (DMVPN) technology
- Zero-touch deployment process for routers

RESULTS

- Improved employee productivity, satisfaction, and retention
- Deployment cost savings
- Reduced environmental impact
- Ability to add new users quickly
- VPN scalability to support thousands of users

LESSONS LEARNED

- Plan deployment to maintain overall network security.
- Large-scale VPN deployment can be achieved with manageable ownership costs.

NEXT STEPS

- Site-to-site VPN
- Support for more user tools such as mobility and TelePresence
- Increased VPN resilience
- Automation of more VPN management tasks

With Cisco's global presence, employees regularly need to collaborate across continents and time zones. Remote network access from home eases the burden on employees who must attend meetings outside of regular business hours. Remote access also provides the flexibility for employees to continue working from home in an emergency, severe weather, or other conditions that prevent them from traveling to a Cisco office. This greater work flexibility provides an extra layer of resilience that can help Cisco continue business operations under adverse conditions.

In the 2008 "Best Places to Work" study conducted by *Fortune* magazine, Cisco ranked #6 overall and #1 for telecommuting options. This study found that 70 percent of Cisco employees work at least 20 percent of their work week at home. Among the categories of teleworkers at Cisco:

- Full-time teleworkers who work from a fixed external site, usually their homes
- Part-time teleworkers who telecommute a few days a week
- Part-time employees who work from home
- Day extenders who work from home evenings or weekends
- Part-time teleworkers, including consultants, who telecommute for specific projects

CHALLENGE

To deliver remote network access to users working at home, in 2001 Cisco IT introduced a software-based VPN solution. This solution provided the necessary security and authentication features that Cisco IT demanded, but establishing a network connection took time and lacked some important features. After the VPN client was loaded onto the PC, users would connect to the Internet, connect to a headend VPN concentrator at the Cisco corporate VPN hub site, log on and authenticate with a one-time password 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 a laptop PC 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.

But for teleworkers who required more sophisticated connectivity at home, the software VPN solution had limitations. The VPN client supported only the PC where it was installed. Other devices, such as additional PCs, print servers, or printers, were not recognized by the network, which limited user productivity.

Another major limitation of the software VPN solution was the lack of support for IP phones and video conferencing, critical items for home offices in a global company. Many employees want to attend meetings that, because of time zone differences, take place when they would prefer to be at home. A good VPN solution would allow them to work from home at these times without the inconvenience of traveling to the office.

With the software VPN client solution, there was no jack on a PC or laptop for connecting IP phones. Cisco Unified Personal 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. For example, if the user sent large file packets over the Internet link while talking on the IP phone, voice quality would often suffer. Voice packets would be delayed and eventually dropped behind the large file packets, causing the voice call to have silent gaps or crackling static sounds.

Deploying a Hardware-Based VPN

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 VPN architecture called Dynamic Multipoint VPN (DMVPN).

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

Preparing for Large-Scale Deployment

The Cisco Security Technology Group and Cisco IT initiated and managed an internal trial of the new hardware-based VPN solution in late 2002. By March 2003, more than 500 Cisco teleworkers were participating in the trial. This trial helped the product group identify issues related to end-to-end connectivity, QoS, and security solutions. Cisco IT recognized issues related to provisioning and managing this solution on a large-scale, for 30,000 or more eventual users.

The deployment issues identified by Cisco IT included:

1. Supporting a mix of technically knowledgeable and nontechnical users
2. Avoiding the situation where employees might use nonstandard hardware or configurations, which would complicate network management and could present a network security risk
3. Simplifying router installation and configuration to allow the solution to be adopted easily by thousands of employees

The options for configuring routers provide an illustration of these challenges. During the initial trial, each Cisco router was manually configured by a Cisco IT engineer before being sent to the teleworker. The engineer followed a lengthy process to generate a configuration, then manually copied the configuration onto the new router. The enormous amount of time that would be required to configure routers in a full-scale deployment was a concern for Cisco IT. A review of industry practices identified several common deployment scenarios:

- Manually configure each router internally and ship it to the user
- Ship routers to a staging facility operated by an ISP, where the routers would be configured and then shipped to the user
- Contract with a company to configure and install the 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. Cisco IT needed new capabilities for the labor-intensive provisioning process and the network management of so many devices.

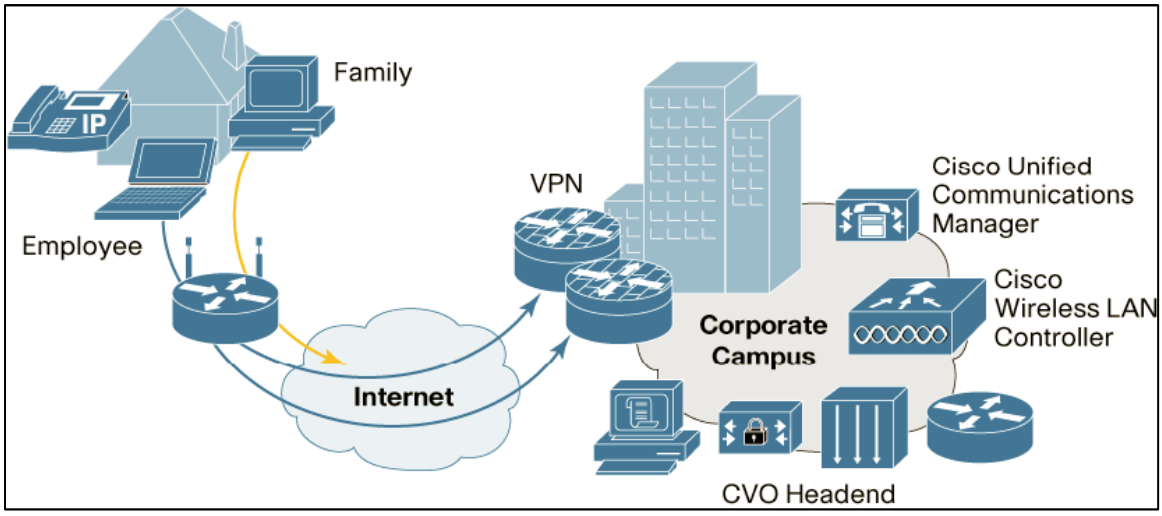
In March 2004, Cisco IT agreed to assume support responsibility for most of the 500 pilot users and take the lead role in developing new router provisioning and management processes. Cisco IT's goals at this point included:

- Secure VPN remote-access service for users
- Global deployment and support model for the routers
- Global management capabilities for all solution components
- Low total cost of ownership for Cisco's deployment of a hardware-based VPN solution

SOLUTION

Cisco IT found a way to meet these goals by adopting the Cisco Virtual Office solution (previously known as the Enterprise-Class Teleworker solution). The Cisco Virtual Office solution provides a secure, encrypted, always-on connection that is easy for an employee to set up and use, and easy for Cisco IT to manage. By providing extensible network services that include wired and wireless access to data, voice, video, and applications, the Cisco Virtual Office effectively creates a comprehensive office environment for employees regardless of their location (Figure 1).

Figure 1. The Cisco Virtual Office Solution Provides Secure VPN Access over the Internet



At the employee's home or remote site, components of the Cisco Virtual Office solution include a Cisco 871 or Cisco 881 Integrated Services Router and a Cisco Unified IP Phone 7965G. These and other user devices access the VPN over a high-speed broadband connection, e.g., DSL, cable, or fiber to the home (FTTH).

The Cisco 871 or Cisco 881 Integrated Services Routers provide secure wireless connectivity in a home office without requiring a separate wireless access point. In addition, these routers support split tunneling, which allows employees working at home to connect directly to the Cisco corporate network over the secure VPN, while the rest of the family can use the same router to connect directly to the Internet. The QoS support helps to ensure that the employee's work-related voice and video traffic receives sufficient bandwidth when family members are using the home network. Although the Cisco 871 router is used by teleworkers in remote offices, the Cisco 881 router also provides the processing power to support a small office with several users.

At the network headend, a Cisco Catalyst® 6500 Series Switch and Cisco 7206VXR routers aggregate and terminate

the secure, encrypted tunnels from each remote site. The headend also supports other VPN technologies such as Group Encrypted Transport (GET) VPN, EzVPN, Secure Sockets Layer (SSL), and Layer 2 Tunneling Protocol (L2TP) over IPSec VPNs, and can effectively serve as a single point of convergence for multiple access technologies.

PRODUCT LIST

Routing and Switching
- Cisco 871 or Cisco 881 Integrated Services Router
- Cisco Catalyst 6500 Series Switch
- Cisco 7206VXR router

Unified Communications
- Cisco Unified IP phone

Security and VPN
- Cisco Security Manager
- Cisco Configuration Engine
- Cisco Secure ACS

In addition, the headend architecture includes the Cisco Security Manager, Cisco Secure Access Control Server (ACS), and the Cisco Configuration Engine applications. Together, these applications define network-wide security policies, verify user identity for authorization, and actively update configurations at remote sites through a zero-touch deployment model.

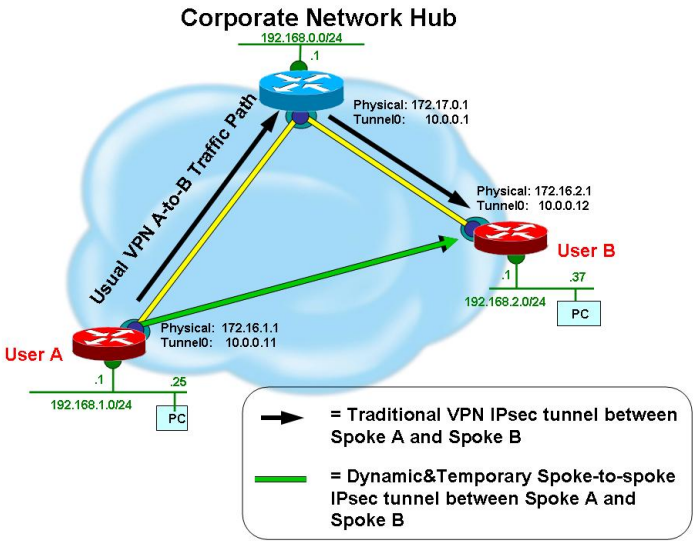
DMVPN Technology Supports Collaboration

The central technology behind the Cisco Virtual Office solution is DMVPN, which provides a scalable, manageable, and secure solution for interconnecting thousands of endpoints to a hub router. With hub-to-spoke DMVPN, the hub router does not need to add new configuration information for every new spoke router, which simplifies the process of adding new virtual office users. Cisco uses this hub-to-spoke DMVPN for the 15,000 routers deployed in its Cisco Virtual Office solution as of mid-2008.

DMVPN also provides the option of spoke-to-spoke connections, which allow home-based teleworkers to connect to each other and directly share data, voice, or video across secure, IPSec-encrypted tunnels through the Internet, without connecting to the Cisco hub router. This design improves network performance and reduces the amount of traffic handled by the hub router and hub Internet access line.

As of late 2008, Cisco was testing spoke-to-spoke DMVPN for employees in China and Latin America (Figure 2). 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 connecting through the nearest Cisco network hub. With this design, DMVPN offers a far more scalable way of building secure, collaborative, peer-to-peer connections over the public Internet.

Figure 2. DMVPN Tunneling Enables Direct User-to-User Connections



Zero-Touch Provisioning Process

With the previous software-based VPN solution, Cisco IT could not meet the demand for new VPN users when a technician could, at best, preconfigure six to eight routers per day. To make the Cisco Virtual Office solution globally scalable, a new type of router provisioning was needed. “Zero-touch” provisioning automates the router configuration process, eliminating the time and effort previously spent by technicians and simplifying router installation for the user (Figure 3). From the user’s perspective, the entire router provisioning process takes only three to four minutes. The following steps are completed by the user for deploying the Cisco Virtual Office solution:

Step 1: Submit a request for VPN service.

Step 2: Receive the Cisco 800 Series router at home.

Step 3: Connect the Cisco 800 Series Router to the existing ISP equipment and connect to the Internet.

Step 4: Enter the URL of the Cisco IT Registrar server into the browser address field (this URL is sent to the user upon manager approval).

Step 5: When prompted, enter the user name and password.

Step 6: Within a few minutes, the Cisco 800 Series Router is fully configured over the VPN connection and the user is notified that the installation process has been completed.

Supporting this zero-touch deployment process for users is a set of related processes in the Cisco network. Steps in these processes include:

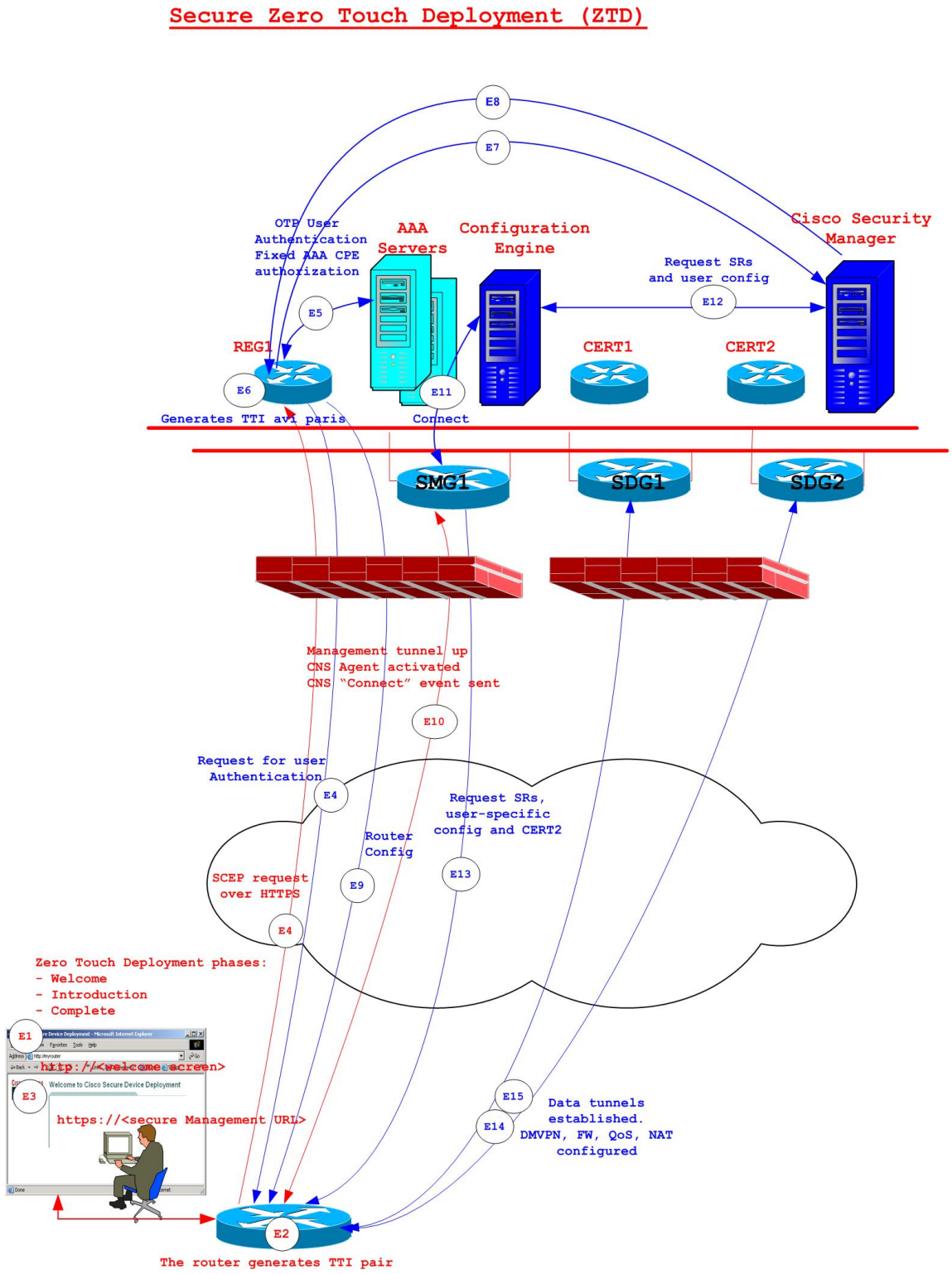
Step 1: Upon approval by the employee’s manager, the Cisco 800 Series Router configuration is automatically processed by the Cisco Security Manager and staged by the Cisco Configuration Engine, making it ready for download when the user connects the router to the Cisco VPN.

Step 2: When the user’s router connects to the Cisco Secure Management Gateway, the router “calls home” to the Cisco Configuration Engine. At that point, the Cisco Security Manager performs the following tasks:

- Pushes the staged security policies to the router, including changing the IP addresses or IP subnet of the user
- Assigns a predefined IP address space for the user
- Applies policies related to IPSec, firewall and user authentication, and QoS
- Applies Network Address Translation (NAT)
- Deploys wireless, IP telephony, and video services to the router if the user has applied and is eligible for these services
- Applies IP service-level agreement (SLA) and Network-Based Application Recognition (NBAR) configurations

When the router configuration is complete, the user logs in, enters a password, and upon successful authentication connects to the Cisco corporate network.

Figure 3. Cisco Virtual Office Solution Provisioning Process



Management Process

The Cisco Virtual Office solution is managed from five global hubs. Data connections are handled by 11 data hubs globally, which use server load-balancing technology to distribute user traffic among Cisco 7206 Router farms.

Several components combine to provide management of the Cisco Virtual Office solution, including Cisco's internally developed enterprise management tool (EMAN), Cisco Security Manager, and Cisco Configuration Engine. EMAN performs resource monitoring, automatic pager alerts, 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, and passes that information to the Cisco Security Manager.

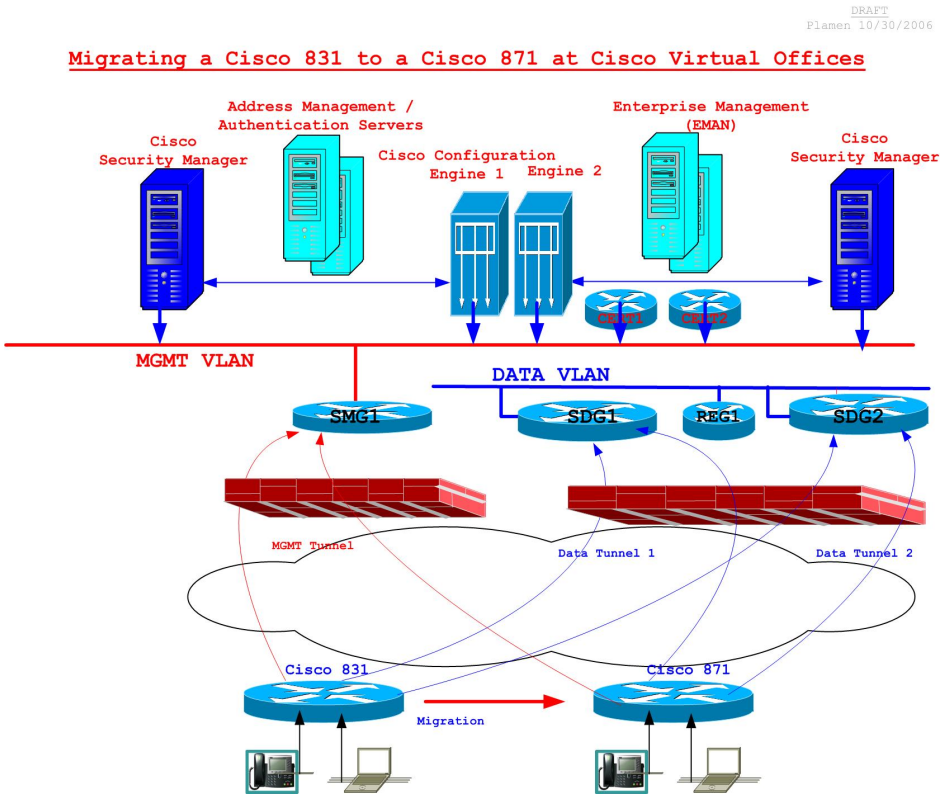
The Cisco Security Manager software manages various types of connections between central servers and remote clients. It is used specifically within the Cisco Virtual Office solution to generate and maintain router configurations and policies. The Cisco Security Manager does not communicate directly with a Cisco 800 Series Router. Instead, configurations and policies created by the Cisco Security Manager are forwarded to the Cisco Configuration Engine. The Cisco Configuration Engine downloads the configuration and policy information to the remote Cisco 800 Series Router. It communicates with the router over the VPN through a management tunnel, which is separate from the two data tunnels.

The Cisco Security Manager and Cisco Configuration Engine also play a major role in ongoing management of the remote routers. During the lifetime of the solution, the user can subscribe and unsubscribe for services or change the service parameters (such as upload speed of the broadband service), move from one location to another, or even migrate from one router platform to another. By using the Cisco Security Manager and Cisco Configuration Engine, all of these operations are fully automated and do not require an IT engineer to be involved in making the necessary router configuration changes.

The user only needs to apply for the router migration or configuration change. Cisco Security Manager will generate a new configuration, which will be sent to the Cisco Configuration Engine. If the router is connected, Cisco Configuration Engine downloads the new configuration to the router. If the router is not connected, the Cisco Configuration Engine stages the configuration and waits for a "call home" event from the router.

Automating these routine operations has proven to be a major factor in reducing the overall operational and support cost portions of TCO for the solution. Automated configuration also simplifies user activity when migrating to a new router, such as the Cisco 831 to Cisco 871 router migration shown in Figure 4. In this case, the user simply submits a migration request. The automated processes recognize when the new router connects to the VPN and update the old and new router management records in the Cisco EMAN system.

Figure 4. Cisco Virtual Office Solution Migration Process from Cisco 871 to Cisco 881 Platform



RESULTS

In August 2004, the Cisco Virtual Office pilot was declared a success and became a full-production Cisco IT service. As of mid-2008, more than 15,000 Cisco employees used the Cisco Virtual Office solution. Even as it supports a growing number of VPN users, Cisco IT is reducing deployment costs with the zero-touch deployment processes: as much as 10 percent for automated router configurations and 5 percent for automated configuration of IP telephony devices.

Through the Cisco Virtual Office solution, Cisco has created a sustainable global deployment and support model capable of meeting the needs of teleworkers worldwide. This model provides global management capabilities that ensure the reliability, availability, and security of the VPN service. “The Cisco Virtual Office solution combined different Cisco technologies. For example, the ability to push policies to remote routers was new for Cisco,” says Plamen Nedeltchev, senior member of the Cisco IT technical staff. “Integrating those technologies and capabilities into a single device while maintaining low total cost of ownership was the biggest challenge of this project. But it was a challenge we met through zero-touch deployment.”

Zero-touch deployment was nominated for Cisco’s internal Outstanding Core Technology Award for 2005 for its contribution to lowering the company’s costs. Typically, deployment and support of a network service represent a large portion of the total cost of ownership. Zero-touch deployment is expected to reduce this cost by 20 percent or more for Cisco’s VPN service and is being applied to more Cisco IT services that require deployment of thousands of configurable devices such as mobile secure phones or PDAs. Cisco IT’s goal now is to expand zero-touch deployment to any device, any service, any location.

DMVPN and the Cisco Virtual Office 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. Among these innovative features:

- Poof of concept for DMVPN
- First use of a public key infrastructure (PKI) within the Cisco IT environment
- First implementation of zero-touch deployment processes
- First fully automated, end-to-end processes for router deployment, provisioning, and management
- First capability for pushing changes and applying security policies to routers in real time without disrupting the user’s connection

The User Experience

Compared to the previous software VPN services, teleworkers have gained significant benefits with the Cisco Virtual Office solution. Because the hardware solution supports an always-on VPN service, employees can use the Cisco IP phone for business calls at any time. To start routine work, a data sharing session, or a video conference, users simply turn on the PC, login, and are immediately connected as if they were in the office. With the continuous router connection to the VPN, the tedious and time-consuming process of establishing a VPN session is eliminated. Working early or late is made easier when working from home, and processing jobs can be set to run overnight.

> “With the Cisco Virtual Office solution, I leave my laptop on most of the time after hours and on weekends. If I think of some small work-related task, I’ll just walk to my home office and do it then.”
>
> **Thomas Herbst, Cisco Virtual Office Solution User**

“There is a significant contrast in how I use my laptop now,” says user Thomas Herbst. “With the Cisco Virtual Office 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 email 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 until I had a working network 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 remembered them.”

In late 2007 and early 2008, Cisco IT conducted an extensive survey of Cisco Virtual Office users to identify the results achieved from the solution. Respondents reported the following key data:

- Employees used the solution to work at home (part-time or full-time) at least three days per work week.
- Productivity improvements while working at home were estimated by employees at 49 percent compared to working in a Cisco office.
- Eliminating the commute to work saved an average of 2.81 hours per employee per week.
- Users gave an average rating of 4.7 (out of a possible five points) for their satisfaction with the Cisco Virtual Office solution.

Combining these factors, Cisco employees who use the Cisco Virtual Office solution achieved a 29 percent improvement in their overall productivity, nearly one-third of the work week gained.

Giving employees the tools to work productively at home also increases their job satisfaction and Cisco’s employee retention. Cisco’s internal survey found that more than 90 percent of respondents gave a high ranking to the value of working at home for the factors of employee retention and satisfaction, flexibility in work schedules, ability to maintain a balance between life and work, and feeling trusted and empowered as employees.

Reduced Environmental Impact

By allowing Cisco employees to work at home and minimize driving, the Cisco Virtual Office solution produces benefits for the environment, as shown in Table 1. Based on a 2008 survey, Cisco expects these environmental benefits to reach nearly 77 million automobile miles avoided annually across the company, with a total yearly reduction of 39,000 tons in carbon dioxide (CO_2) emissions.

Table 1. The Cisco Virtual Office Solution Reduces the Company's Environmental Impact by Reducing Employee Travel.

Cisco Green Environmental Factor	Average per Employee / Per Year Result (as of Early 2008)	Estimate for Cisco 2008 (Based on 15,000 Employees)
Miles avoided for employee commuting	5135 miles	77 million miles
CO2 emissions reduced	2.5 tons	37.5 thousand tons
Reduced gasoline consumption by employees	257 gallons	3.8 million gallons
Gasoline cost savings (US$3.50 per gallon)	US$900	US$13.5 million

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 Virtual Office solution allows me to work with Europe 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 Virtual Office 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. "The main value of the Cisco Virtual Office 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, a Cisco engineer. "With the software VPN, I had two PCs sitting on my desk that couldn't talk to each other, which was inconvenient when I needed to copy files between them."

Having office resources at home provides a more flexible work environment, which can increase an employee's job satisfaction. The Cisco Virtual Office solution also allows employees to work easily when away from an office location, in another county, another state, across the country or globally, if needed.

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

The Corporate Experience

Cisco has conservative policies for network security, with a consistent posture of low risk-taking. The Cisco Virtual Office solution minimizes network risks 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 Cisco Virtual Office solution simplifies management of the VPN security environment and allows comprehensive analysis and automated decision-making for responding to network threats.

The Cisco Virtual Office 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 and password before applying for teleworking service. When users set up the router, they must have a one-time password to configure the device. Then, the user must enter a valid password whenever they log in to the Cisco network. Finally, the router itself must be authenticated by the system during login.

Other security features in the Cisco Virtual Office solution include the ability to automatically disconnect a terminated employee within seconds. If a user attempts to recover a password or changes the host name of the router, the remote router will lose its private keys and any attempt to access the Cisco network will fail.

Cisco IT Experience

The provisioning and management capabilities of the Cisco Virtual Office solution greatly benefit Cisco IT. Zero-touch deployment reduces Cisco IT's involvement in router configuration and significantly eases deployment scalability because 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 Cisco Virtual Office solution, Cisco IT managed about 2400 routers in the worldwide Cisco network and added up to 10 per month. With zero-touch deployment, DMVPN, and integrated router and security management, Cisco IT can add more than 1000 routers per month to the VPN while maintaining low total cost of ownership.

"Cisco IT has already subscribed more than 15,000 employees to the Cisco Virtual Office solution, and we anticipate that more than 30,000 Cisco users will eventually decide to use the service," says Nedeltchev.

LESSONS LEARNED

Cisco IT staff has identified the following lessons learned from its internal deployment of the Cisco Virtual Office solution.

VPN security design. The security of VPN services over the Internet is a major, ongoing factor for protecting the intellectual property of the enterprise and for maintaining high availability of corporate network resources. This level of security requires all architectural decisions for the Cisco Virtual Office solution to be in compliance with non-compromised security rules and auditable security policies.

Zero-touch deployment. 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.

Managing TCO. Large-scale VPN deployments can be achieved if you maintain a manageable TCO. The zero-touch deployments, automation of routine router operations, and reusing the existing network management components are the major factors that have helped Cisco IT reduce the TCO for the Cisco Virtual Office solution.

Monitor service-quality factors. Providing an enterprise-class VPN service for employees who work at home means maintaining preemptive capacity planning, and controlling the IP SLA for every end device and service. The availability of the broadband service, the one-way latency, the service error rate, jitter levels, and the Mean Opinion Score (MOS) for voice calls are the major factors that should be measured for determining overall quality of the home-office service.

NEXT STEPS

Cisco IT expects to adopt several planned enhancements to the overall Cisco Virtual Office solution.

New-generation very small office. Recognizing that small offices can also benefit from VPN connections to a corporate network, Cisco expects to extend the Cisco Virtual Office solution to support access by multiple users within a site. This design will also allow site-to-site connectivity among offices without going through a central network hub. Cisco IT would use this design for sites such as small offices, permanent presence of Cisco employees at customer premises, and early connection of newly acquired companies to the Cisco network.

User mobility. To meet the needs of highly mobile employees, the Cisco Virtual Office solution will support VPN access from devices such as PDAs and selected mobile phones. The mobile phones and services will be deployed with zero-touch deployment and will provide a full range of services such as WiFi connectivity, use of dual-mode (IP and cellular) mobile phones, VPN, email client, and the employee's Cisco Unified Mobile Communicator software. Employees will also enjoy access to more productivity tools, such as Cisco TelePresence, while working from home.

VPN resilience. Giving employees access to the corporate network is now considered a business-critical service at Cisco, especially for enhancing business continuity. To increase the resilience of VPN services, Cisco is developing a

fully redundant VPN design that will allow automatic switching of user connections among hub sites.

Increased automation. Based on its success with the Cisco Virtual Office solution, the zero-touch deployment concept is being adapted for other Cisco products and solutions, such as IP telephony devices. The Cisco Security Manager and Cisco Configuration Engine will be positioned to address the management needs of other Cisco network segments, which will reduce deployment time and costs for new services.

FOR MORE INFORMATION

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.
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.

