How Cisco IT Provides Secure and Flexible Remote Access for Mobile Employees and Home Offices

Scalable VPN technology boosts employee satisfaction, improves enterprise business resilience, and lowers remote-access costs.

Cisco IT Case Study / Security and VPN / Scalable VPN Remote Access: This case study describes Cisco IT's internal deployment of Cisco VPN Client within the Cisco global network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

In August 2001 the Cisco Systems® IT remote access group faced a crisis. Their primary high-speed remote access solution in the United States, based on DSL, was about to disappear. The primary service provider, Rhythms NetConnections, had filed for bankruptcy in August 2001 and promised to provide service for another month; after that time, the more than 9000 Cisco® employees who depended on the Cisco IT DSL service would be without service. The remote access team faced migrating 9000 users in a single month, and they knew from experience that migrating to other standard remote access service like ISDN or another managed DSL service would be very costly, and take more than 10 times the staff they had available.

"But this crisis proved to be the best thing to happen to Cisco IT," says Dave Holloway, manager of the Remote Access Services group in Cisco IT. "It forced us to consider other options, and forced us to accelerate our migration to a VPN solution. That single move has not only saved us money, it's improved client service and client satisfaction, and paved the way for new services we couldn't have considered with our other remote access offerings."

Over the past few years remote access VPN has become the primary remote access mechanism for Cisco employees who are telecommuting from home or traveling, and who require access to the corporate network. Cisco IT has been supporting a remote access VPN solution with Cisco VPN Client software for more than three years. This software VPN client installed on users' laptop computers provides remote access to the Cisco corporate network with relative ease and enhanced security. Users locate and manage their own Internet access for this service, and are reimbursed by their department for their Internet access charges. This case study discusses in detail the business advantages to Cisco of a robust remote access solution like our Internet-based VPN, and then details the background, service deployment issues, support issues, cost savings, and other benefits of the VPN migration, and some future plans for remote access within Cisco.

BACKGROUND: BUSINESS ISSUES AND HISTORY

Remote access has been seen as a critical part of Cisco IT's support for our end users, and has provided numerous benefits to both end users and to the corporation. Cisco IT has been providing remote access connectivity to our end users for more than a decade, and we have always strived to provide the best possible technological tools to support ubiquitous high-speed access to our end users. Moving to a high-speed Internet-based VPN remote access solution has enhanced the many benefits of previous remote access solutions and has added new benefits. This section examines those benefits, and reviews the history that brought Cisco IT to our current remote access solution.

Business Issues with Remote Access

Most companies cite improved productivity and greater employee satisfaction as the benefits for supporting a robust

remote access solution, and these are certainly sufficient reasons for providing good remote access to employees. But in addition to these benefits, Cisco IT has noticed that a good high-speed remote access solution does more—it enables a company to be truly global, and provides the company with additional flexibility to meet emergencies. In addition, Internet-based VPN remote access has reduced our support overhead, improved security, and reduced our per-user costs significantly. This section details those benefits.

Client Productivity

Remote access, especially high-speed remote access, has always been seen as a fundamental tool to improve employee productivity within Cisco. "We usually log on (to the Cisco intranet) in the morning, before going to work; and then log on again in the evening after we come home, for another hour or two each day," says one Cisco employee. In the past when slower dialup remote access was the only service option, employees tended to dial in to upload and download e-mail after hours. But high-speed remote access means that employees can perform almost all work functions from home or from the road, such as accessing shared network files or conducting collaborative meetings, and Cisco employees have embraced these capabilities. For many employees this translates to an additional 10 to 40 percent productivity per employee per day. In addition, some work can be done more easily at home. "I get my most productive work done at home. I can write steadily without losing my focus, without interruptions or phone calls," says Lew Thorne, a project manager within Cisco IT.

In late 2001 Cisco IT migrated its user base from a Cisco IT-managed DSL service to a client-managed VPN service. Rather than supporting only those employees who were in the Rhythms DSL area, the service now supports users wherever they can find an Internet service provider (ISP). This move has allowed many more Cisco employees to improve productivity using high-speed Internet services—in 2001 Cisco had 9000 DSL users and now, in 2003, Cisco has more than 23,000 VPN users.

Client Satisfaction

Cisco employees find it much easier to balance their work and home lives with high-speed remote access, and this improves morale and makes it easier to retain valuable employees. "Last week I had to take my two-year-old daughter in for a doctor's visit and immunization shots," says Ron Matz, a Cisco Web developer. "I was able to log on to Cisco and work for a few hours before taking her to her doctor's appointment, and then work later that night to make up for the lost time. Telecommuting from home also gave me more time to be with my daughter during the day." He later added, "Time at work is valuable for maintaining connections with your co-workers, but being able to work from home gives me more time to see my family. This is a real quality-of-life issue for me, and I would be less likely to take a job with a company that didn't provide good remote access." Employees can work from home to be with sick family members, to provide emergency child care, or just to be home for service installations or deliveries that can't be done on the weekend.

In addition, reliable high-speed remote access has allowed Cisco to retain employees who needed to or wanted to move away from main Cisco locations for personal reasons like family issues or cost of living. Their ability to find high-speed access from almost anywhere in the world has allowed them to remain with the company, and has allowed Cisco to continue to benefit from their expertise and hard work.

Migrating from a Cisco IT-managed DSL service to a client-managed VPN service has also allowed Cisco employees to get better service, by letting them locate the best possible high-speed access available at their location. Explains one Cisco employee: "We share information among ourselves about the best ISP in my area—the ISP with the highest bandwidth, or the best service record, or whatever. When Cisco IT allowed me to choose my own remote access method, I chose a local cable provider. I'm getting between 1- and 2-Mbps download speeds, much faster than my previous DSL service could provide."

Globalization

Being a global company requires more than simply having global presence. A global company must also enable its global employees to work together effectively. When the distance between global sites is removed using normal

voice and data network tools, there still exists another barrier to effective global collaboration—time zone differences. "In my role as a global program manager, I have to constantly host or attend conference calls at all times of the day," says Oisin Mac Alasdair, a global program manager based in Sydney, Australia. "Due to the differing time zones, I will typically get up at 5 a.m. to work with my American colleagues, and often work late into the night to ensure I'm online for some of the working day in Europe. Broadband access at home is an invaluable tool, in that it provides me with the same functions at home as I have in the office." Oisin notes that many of his colleagues in different theaters experience the same benefits. "Using Cisco technology, such as broadband VPN solutions, voice-over-IP services in the Cisco AVVID (Architecture for Voice, Video and Integrated Data) suite, and Cisco Aironet® wireless LAN technologies, I'm capable of having a fully productive day, with full access to all the corporate services essential for me to do my job successfully, without having to spend 20 hours plus per day at my desk. My colleagues and teammates do the same, whether they're in San Jose, Sydney, or London." Oisin says that, "whilst we can't change the march of time, we can certainly ensure our staff juggle both their working and personal lives" in a successful and productive way. "It really is an advantage," says Oisin. "I honestly couldn't do my job without it." Migrating from a Cisco IT provided DSL service, limited in scope to only certain parts of the United States, to a client-selected VPN service has allowed employees worldwide to create their own home offices. The VPN service connects them at high speeds to the corporate intranet, letting them work far more conveniently from any location, at any time.

In addition, the larger number of employees working from home has begun to transform the meeting behavior of Cisco employees, making meetings easier and more productive for global teams. In prior years most meetings at Cisco, especially those held at corporate headquarters in San Jose, California, had most people meeting face to face in a room, with an audioconference bridge set up for a few team members from around the world to call into.

Because most employees at corporate headquarters rarely experienced meetings from an audio bridge, they didn't realize how often they failed to accommodate the needs of remote employees—speaking clearly, soliciting input from the team members on the bridge, sharing documents or presentations using collaborative software (such as IBM Lotus Sametime Connect, OpenText Livelink, or Microsoft NetMeeting), verbally clarifying whiteboard drawings and body language, etc. Remote employees, usually in Europe or Asia, often felt they didn't get the full value of meetings they attended with employees from corporate headquarters, and their frustration led to less productive engagement across global teams.

Today, most employees from corporate headquarters spend more of their time working remotely, and they have become much more aware of meeting behavior issues that hinder participation of remote attendees. Because of this heightened awareness, an increasing number of team members are quick to ensure that meetings work equally well for local and remote employees, and global teams have become more numerous and productive.

Flexibility

On December 5, 2002, an unusually severe ice storm struck the Cisco site at Research Triangle Park, North Carolina. Buildings lost power, and it was too dangerous for most people to drive to work. The effects of the storm lasted for three days. In the past this would have resulted in lost work for more than 1000 employees for those three days. But because almost all employees were already used to using their high-speed remote access, they were able to be as productive while working from home as they would have been at work.

In April 2003, an outbreak of Severe Acute Respiratory Syndrome (SARS) curtailed travel for Cisco employees throughout parts of Asia. "In China at the height of the SARS period, (mid-April to mid-May), most of Cisco's 800 staff were working from home. Despite this, the organizational productivity was minimally affected, although sales productivity did suffer somewhat. The role of relationship in Chinese business plays an important role. Customers have an expectation that their suppliers will meet with them face-to-face. During the SARS period, however, there was a national interest in avoiding such face-to-face meetings, so utilization of tools such as videoconferencing increased dramatically. During some of the busiest days, the network traffic across Beijing's public backbone increased by a factor of three. At the onset of the SARS period, we were at the beginning of the Cisco IP SoftPhone

rollout in China. In partnership with the client, the project was fast-tracked and early rollout meant that IP SoftPhone played a major role in mitigating possible productivity loss caused by minimal staff working from the office," says Greg Dixon, Cisco China's IT manager in Beijing. "When we were preparing contingency plans at the beginning of SARS in anticipation of office closures, we were surprised how little we had to do because we were already positioned well in terms of broadband VPN from home. SARS demonstrated to most organizations the complexity of disaster planning. It was certainly a good lesson in the value of voice-data convergence and VPN technology over an IP network. Now that SARS concerns seem to have subsided, with business recovering to more normal conditions, many customers are thinking about how they can also be better prepared. They see Cisco as a model example and we find ourselves increasingly talking to them about what we have done."

Remote access provides added flexibility during a crisis and also for everyday activities. “My commute can last two hours each way during rush hour,” says one employee. “I do most of my work from my home office and come in to work at the office one day a week. I get more work done this way, and save myself four hours of driving every day.”

Employees who travel can access e-mail and upload and download small files over simple dialup connections using the VPN connectivity. However, a growing number of hotels and coffee shops are providing high-speed Internet access, either free or for a small charge, and more Cisco employees are taking advantage of this to be able to work more productively while traveling.

The widespread availability of Internet-based high-speed remote access is also providing Cisco employees with a platform to try new services. Some Cisco employees have an IP phone or SoftPhone extension in their home office, allowing them to make calls on the Cisco IP network. A few Cisco employees are using IP video cameras to set up videoconferences with other teams within Cisco from their home office. These and other planned services are discussed in more detail in the “Next Steps” section of this case study.

Manual Support

Supporting a remote access service can require a large amount of labor-intensive effort. “When we were providing private DSL access to 9300 Cisco employees, we had 10 engineers on staff in our San Jose campus working full time in our remote access team. We had outsourced most of the setup to Rhythms, which meant that Rhythms’ engineers were going to employees’ homes to set up the DSL routers and test the DSL access, taking trouble calls when there were problems, and sending technicians to employees homes to resolve some problems. This allowed us to refocus our efforts from solving problems to managing Rhythms. But our own Cisco IT remote access engineers still had to provide service to employees who weren’t in the Rhythms service area, so we still had to support employees on Frame Relay and on ISDN, and we had to set up and support their routers ourselves, which is time intensive. We also maintained a large dial-in access service locally. With about 700 DSL users being added or disconnected each month, we still had to work out bill reconciliation and service closings with Rhythms, which also was time consuming,” says Dave Holloway, Cisco IT remote access manager. “Now that almost all Cisco employees provide their own broadband VPN remote access service, we don’t do installations or service calls, and we don’t do bill reconciliation. And we’ve moved most of our engineers on to more productive work within Cisco. We now have two contractors and one engineer in our San Jose campus doing all the remote access work we need, and much of that is now devoted to proactive planning rather than to reactive maintenance.” That emphasis on proactive planning is discussed in the “Next Steps” section of this case study.

Security

“With Rhythms handling service closings for us, it took about two to three days to close out an ex-employee’s remote access service. During that time they could still access our network after they’d been terminated, and that was a security risk for Cisco,” says Dave Holloway. “Now that we’ve migrated to an Internet VPN access service, we don’t have to close down an account; the ex-employee can choose to do it if they want. All we have to do is close out an ex-employee’s access from the authentication, authorization, and accounting (AAA) server, which we can do in less than 24 hours.”

Cost

The cost to provide user-managed VPN service is about half that of the cost to provide Cisco IT-managed high-speed access service. The cost for each Cisco employee to buy their Internet access depends a good deal on their location and the type of Internet access available in their area (these can include ISDN, DSL, cable, or leased lines), but it still remains about half the cost of Cisco-provided DSL access. Employees are reimbursed by their departments, when possible, up to a preset limit. So, in a direct comparison between the Cisco IT-managed remote access DSL service and user-managed Internet VPN service, the VPN service provides immediate per-user savings. In addition to these cost savings, the reduced management costs saved Cisco even more. The costs of migrating to VPN services late in 2001 were complicated by other factors, all of which are detailed in the "Savings" section under "Results" later in this case study.

History

Cisco IT has been supporting employees' remote access needs with various technologies for more than a decade. We have strived to provide the best possible remote access service based on the then-leading technologies, which have evolved from asynchronous dial, ISDN, Frame Relay or other protocols over dedicated circuits, managed DSL, and most recently, VPNs. This section provides a brief history of the various remote access solutions supported by IT over the last 10 years.

In 1993 asynchronous dial was the first widely deployed remote access solution offered by IT. At that time, users dialed into modem pools in San Jose, California. In 1995, San Jose became the first Cisco location to be supported with Cisco AS5100 universal access servers and dial software on the clients' PCs. The service was extended to Research Triangle Park North Carolina and other global sites based on the expansion of Cisco locations there and on the east coast of the United States. Over time the Cisco AS5100 access servers were upgraded to Cisco AS5200 universal access servers and a toll-free 800 service was introduced nationwide in the United States. The first international rollout of asynchronous dial access was done is 1998 with Equant, providing remote access to almost all Cisco employees worldwide. Still, the bandwidth limitation of dial access continued to frustrate our end users, and Cisco IT introduced higher-speed remote access.

In 1996, ISDN was rolled out to the first few users supported by a variety of end-user equipment: Cisco 700 Series ISDN access routers and Cisco 3600 Series multiservice platform routers, but primarily Cisco 800 Series routers. This ISDN service was eventually expanded to a user base of about 10,000 clients. However, this solution had several limitations, including increased total cost of ownership based on higher management costs and higher vendor costs. Cisco IT management costs were high because Cisco IT remote access engineers had to manually configure and test each end-user Cisco 800 Series Router for installation, and to resolve problems. In addition, users incurred some high ISDN bills when connecting for longer durations. Because most of the service providers charged for ISDN services based on connection time, it was proving to be an expensive solution. Most users were remaining connected longer than they had with asynchronous dial because of the improved performance, and a few users connected for most of the day for several reasons, the most notable being Windows 2000 performing frequent DNS resolution and keeping up the link indefinitely. "During the first few months of the Windows 2000 rollout, Cisco IT's ISDN costs almost tripled and we had to identify workarounds to get the ISDN bills reduced," says Plamen Nedeltchev, lead engineer in the San Jose remote access team. Cisco IT began looking for lower-cost alternatives.

Frame Relay was rolled out as an alternative for ISDN users with need for long access hours where ISDN had high access costs. Cisco IT had to partner with some service providers for providing Frame Relay connectivity to user homes. There were limitations with the availability of service—many Cisco employees could not get access to Frame Relay service and the costs went up when the user was more than 30 miles from the central office of the service provider. As with ISDN, the Frame Relay needed more hours for Cisco IT remote access engineers to provide deployment, operation, and management of the service. The clients were supported on Cisco 1000 Series routers, Cisco 1600 Series routers, Cisco 3600 Series multiservice platforms, and Cisco 4000 Series routers. Although Frame Relay service is not billed by the hour, it is still somewhat expensive, so the Frame Relay service was

extended to little over 300 users within Cisco.

With the dramatic growth of the Internet and the advent of broadband access becoming available to homes with DSL and broadband cable, IT started to work with various service providers and multisystem operators (MSOs) to provide broadband access to homes. The biggest challenge with providing Cisco employees with a managed DSL service was that IT had to carefully evaluate multiple vendors that varied in the size and locations of their service areas (and thus the number of Cisco employees they could reach), the service level agreements they could commit to, and the cost of the service they could provide. Our goal was to provide the best service to the most employees at a reasonable cost to Cisco. Rhythms Communications was chosen to be the partner to provide private xDSL connectivity for Cisco remote access users within the United States. The Rhythms DSL service was effectively a "private" DSL service offering direct virtual circuit connectivity into the Cisco corporate intranet. The first clients were supported in 1998 with Rhythms providing private DSL service to our clients and dedicated 45 Mbps leased line DS3's providing connectivity between Rhythms and the Cisco intranet. Employees connected to this DSL network with Cisco 600 Series routers and later migrated to Cisco 800 Series routers. Cisco IT's remote access client base was expanded to more than 9000 users in the United States.

CHALLENGE

In 2001 after many of the DSL companies started going out of business, so did Rhythms Communications. Even as IT was looking for backup service options to the managed DSL service, Rhythms filed bankruptcy and they recommended that Cisco IT migrate our user base of more than 9000 remote access users to a new service, with very short notice. "It was November 2000 and we had little more than two weeks for migrating more than 9000 DSL users to an alternate service," says Lainie Van Doornewaard, technical lead for DSL with the remote access team in IT. She adds, "Migrating users to remote access VPN was the best available option at that time so that IT could get away from the costly managed service model."

With the bankruptcy of Rhythms in 2001 and the continued need for more "anytime and anywhere" connectivity, Cisco IT reviewed different options and selected a new model: user-managed services such as VPN where the user would be responsible for providing their own connectivity to the Internet, leaving Cisco IT with the responsibility to provide and support VPN connectivity from the Internet gateway to the Cisco corporate network. This option offered employees several advantages, most notably the far wider reach of Internet access. This wider reach allowed far more employees to take advantage of the new remote access service, and the number of remote access users in the United States more than doubled from 10,000 to more than 23,000 users. In addition to the 23,000 Internet VPN users, there are about 200 Frame Relay users, 1200 ISDN users, 30 T1 users, and 200 managed DSL users with SBC. Most of these additional clients are users who are unable to get any type of broadband access to their home and hence cannot use the user-managed VPN. Globally, Cisco employees still have access to asynchronous dial supported by partnering with Equant and iPass and using VPN and Layer 2 Transfer Protocol (L2TP) from those vendors for connectivity to Cisco.

SOLUTION

The Cisco IT remote access group had been testing VPN-based remote access services for several months, and was prepared to migrate its user base from the service provider managed service model to a user managed model. This user managed model required the user to take over both the ownership of and responsibility for managing their Internet connectivity, as well as paying for the one time installation and monthly charges (which can be reimbursed by the company with management approval). Cisco IT's responsibility was reduced to supporting the users' ability to securely connect to the corporate network. In addition, IT has provided tools to support the installation and configuration of the VPN client software and provides ongoing support for issues with the VPN connectivity.

Service Introduction

From 1998 until 2000 Cisco IT was still deciding on the best remote access VPN strategy. We were looking into

OEM products from companies such as IRE and RedCreek to provide secure remote access service using IP Security (IPSec) functions into Cisco VPN products. With the Altiga acquisition in early 2000, Cisco strengthened its remote access VPN portfolio. At about the same time, Cisco also acquired Compatible Systems. After careful testing and evaluation, IT decided to choose the Altiga line of products to support our internal enterprise VPN deployment, and the Compatible Systems VPN solutions were adapted for service provider needs. Cisco IT worked closely with marketing and the business units, testing and improving the VPN products (the software VPN client and the Cisco VPN 3060 concentrators), making sure that they could be managed easily and could scale to full enterprise deployments.

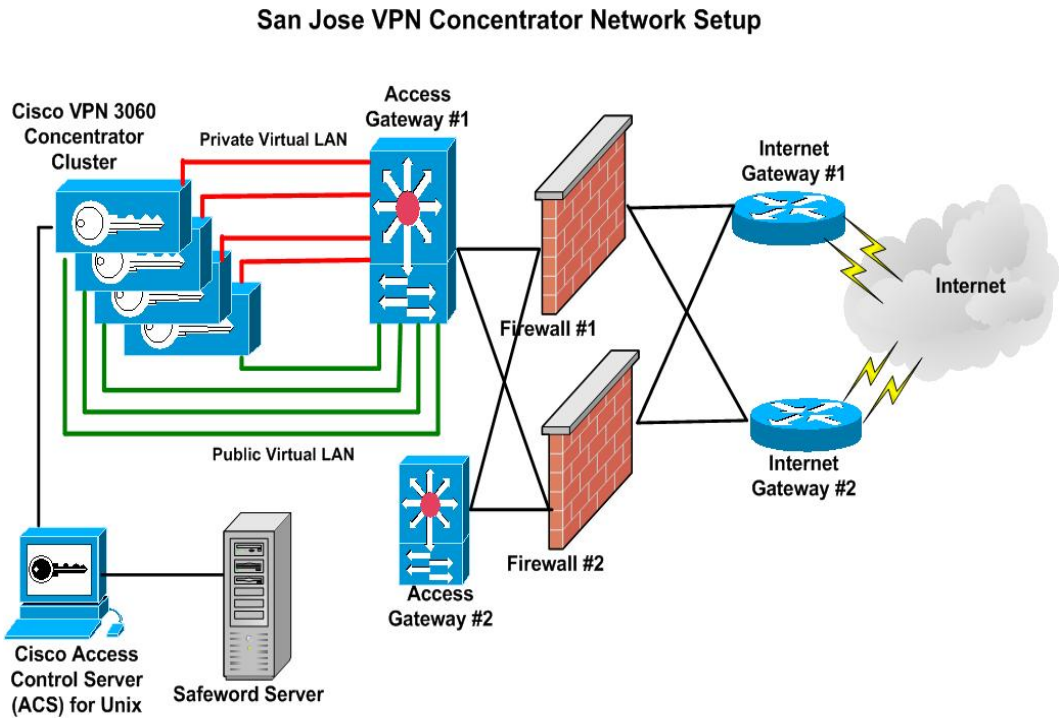
The Cisco IT VPN deployment plan included lab testing of both the software and hardware VPN products, a limited user trial, and extended pilot before moving into production deployment. Cisco IT deployed Cisco VPN 3060 concentrators to all Cisco locations with Internet connectivity, in pairs or (in the case of San Jose, California) in a group of four. These Cisco VPN 3060 concentrators were deployed in San Jose California, RTP North Carolina, Amsterdam Netherlands, Tokyo Japan, and in Sydney Australia. Chelmsford Massachusetts, Tel Aviv Israel, Singapore, Richardson Texas, and Hong Kong China were later added to provide more local VPN headend support (see Figure 2).

The VPN service was first introduced as a limited user trial on September 5, 2000. The first version of the Cisco VPN Client tested was version 2.5, but at the time this version did not support the Windows 2000 platform, which was to become the Cisco Windows PC platform standard within a few months. Engineering built an interim build with version 2.6 that supported Windows 2000 platforms for IT before the Cisco.com version of 3.0 was deployed. Version 3.0 was the first official build to support Windows 2000 PCs. The concentrator features for version 3.0 included support for load balancing through concentrator clustering and Secure Shell (SSH) support for management.

Cisco IT has identified the following prerequisites for any user requiring VPN service:

- **Connectivity to the Internet—**It became the responsibility of the user to get their Internet connectivity from their selected local service provider. IT does not have control over the ISP selection process and it merely provides a reference to the list of service providers available in a particular region. Cisco IT does not negotiate any service contract or special corporate deals with the service providers and it is the responsibility of the user to pick the right ISP that suits their needs. Cisco employees were quick to educate themselves, however, about the issues involved in selecting the best ISP in their area, and shared this information through e-mail on a regular basis.
- **SofToken or DES Gold card account—**Cisco Information Security requires Cisco employees to use a one-time password to access Cisco intranet services across the Internet. This requires a user to have an existing SofToken or DES Card account. Both SofToken (a PC application) and the DES Gold card (a hardware card carried separately by the employee) require the employee to enter a password, and then they generate the one-time password required by the VPN security access control server. Because of associated costs with DES cards, SofToken is recommended for users unless there is a need to connect from more than one computer (SofToken can only be loaded on one computer at a time).
- **Windows operating system—**Currently, Cisco IT supports only the Windows version of the Cisco VPN ClientSoftware, and hence the remote access user should have a Windows PC to connect to the corporate network. VPN support for non-Windows clients is being tested. The Linux version of the VPN client is currently limited to pilots in the Americas and EMEA theaters, without full production support. Full production support will be available at the successful conclusion of the current pilots.
- **Entitlement and reimbursement (optional)—** With management approval the client can reimburse their ISP service installation and monthly charges through Cisco's internal chargeback tool. Cisco reimburses to a maximum of $500 for one-time installation charges and $100 for monthly service charges.

Figure 1. San Jose VPN Headend Architecture



Network Architecture and Design

The network architecture for the remote access VPN network for San Jose is shown in Figure 1. This diagram presents the essential components of the VPN headend setup and does not contain all components of Cisco IT's Internet services architecture. Other sites with VPN headend capability have similar architectures or a subset of the components of the San Jose setup. Smaller locations have two VPN concentrators, and some smaller locations have a single access gateway.

Some of the technical details of the architecture are explained in the following paragraphs about network connectivity, load balancing, security, split tunneling policy, client support, and management.

Network connectivity—The Cisco VPN 3060 concentrators connect to one of the corporate Internet access gateways. Both the public and private interfaces of the concentrator connect to the same gateway. This is due to a current limitation of the Cisco VPN 3000 Series Concentrator—the Cisco VPN 3000 Series Concentrator is limited to three interfaces and hence duplexed redundant path pairs between the concentrator and the access gateway layer cannot be provided. The access gateway connects to the backbone routers that connect to the firewalls protecting the internal network. These firewalls have ports UDP 500 (for ISAKMP), port 50 (for ESP) and UDP 10000 (for IPSec for UDP) opened for the concentrator virtual IP address. The concentrators are connected through Fast Ethernet to the access gateway and configured with default static routes to that access gateway. The network design called for using static routes using the Cisco IT standard Enhanced Interior Gateway Routing Protocol (EIGRP) rather than using Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) with the VPN concentrator network, for simplicity with regard to configuration and support.

Load Balancing—The design in San Jose California consists of four Cisco VPN 3060 concentrators in a single cluster configured for load balancing with the Cisco IT VPN solution. Each of the concentrators is configured for the same priority value, so that they are equally load balanced. This ensures that the load on the concentrators is equally distributed.

Security—Cisco IT's corporate encryption standard is Triple Data Encryption Standard (3DES), and this level of encryption is deployed within the VPN service. Both IT and Corporate Information Security (Infosec) teams are

evaluating the use of Advanced Encryption Standard (AES) as the encryption algorithm of the future. Users are required to authenticate with a one-time password provided with a SofToken application or a DES Gold Card. The concentrators are configured to authenticate users with the Cisco Secure Access Control Server (ACS) for UNIX. Currently the UNIX version of Cisco Secure ACS 2.5 is supported and there are plans to migrate to Cisco Secure ACS for Windows with the VPN solution. The Cisco Secure ACS is configured to point to the Safeword server for one-time password authentication. Currently outbound VPN is not supported by Cisco IT to comply with Infosec policies When a need arises where VPN connectivity must be established to a customer or partner from the Cisco network, a case is opened with Infosec and outbound IPSec is permitted based on the strength of that business case.

Split tunneling policy—Split tunneling is the feature that controls the flow of the users' Internet traffic when they are connected to the corporate VPN, allowing the user's corporate traffic to travel through the VPN tunnel into the corporate intranet, and splitting off the user's public Internet traffic to travel directly to the Internet without burdening the corporate intranet gateway. Infosec's policy is to disable split tunneling, because it provides an insecure path (temporary) between the Internet and the corporate intranet. By disabling split tunneling, all the user traffic will flow through the Cisco corporate ISP gateways, adding additional traffic to the gateway but removing a security risk. Split tunneling is essentially a traffic management feature and not a network security feature. The VPN product team suggests turning off split tunneling where security is of primary interest, as opposed to bandwidth limitation, because turning on split tunneling exposes the client to Internet attacks, Trojans, worms, and viruses. This "no split tunneling" policy is controlled from the VPN concentrator by means of Mode Configuration push and cannot be modified by the end user.

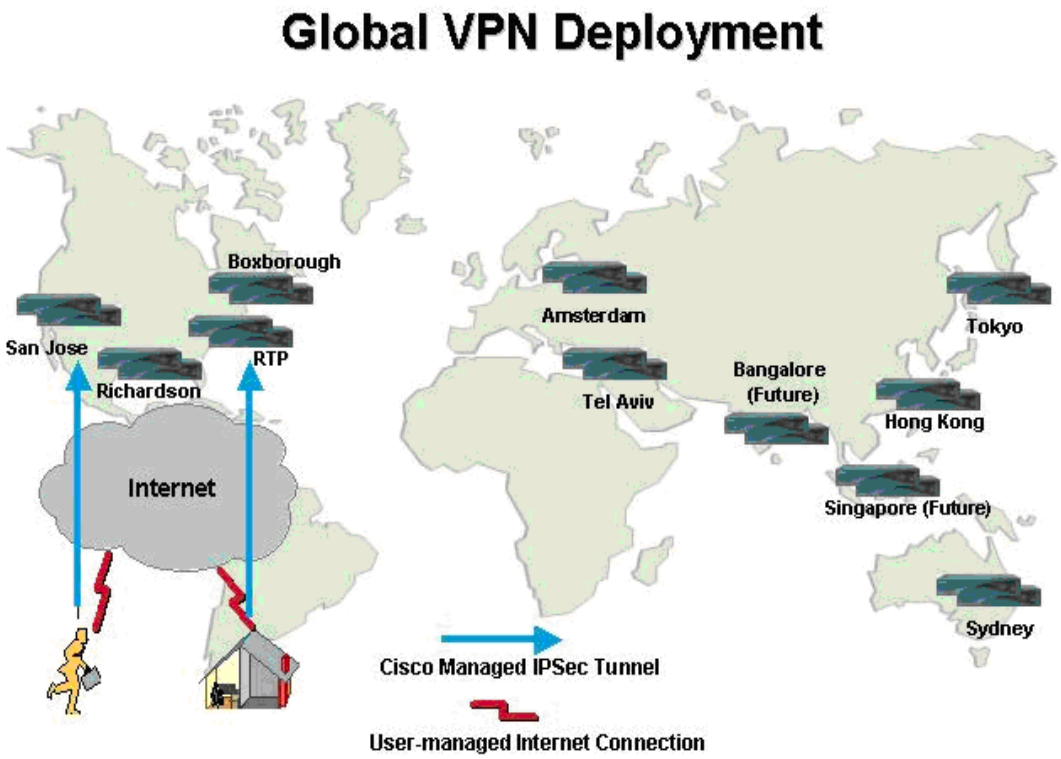
Addressing—The Cisco IT VPN solution uses the Cisco mode configuration support, which is used to control policies from the headend and also to manage connection information from a central location. IP addresses to the VPN clients are assigned from the central address pools configured on the concentrators. The access routers are configured with static routes pointing to the VPN headend concentrators for their respective address pools.

Management—Cisco IT engineers access the concentrators using either SSH and Secure Sockets Layer to provide maximum security. Monitoring the concentrator is provided through EMAN (Cisco IT's Enterprise Management tool) for availability, load, performance, and other statistics.

Support

The Global Technical Response Center supports VPN as a lower-priority (Priority 4, or P4) service, which has a 2-business-day response. A major outage with the VPN service that is not limited to an individual user is a P2 service. The Cisco IT remote access group also maintains several user-support documents providing information to help guide ISP selection, manage VPN service, configure home networks to work with VPN, explain security and billing policy, and provide answers to other frequently asked questions.

Figure 2. Global VPN concentrator locations



RESULTS

Today users can access the corporate network from any location that has a public Internet connection. This includes wired connections and the increasingly popular wireless hot spots at airports, restaurants, hotels, and other public areas. By July 2003, the Global Remote Access VPN solution is supported with nine core concentrator sites in San Jose California, in Research Triangle Park North Carolina, Richardson Texas, Boxborough Massachusetts, Sydney Australia, Amsterdam Netherlands, Tel Aviv Israel, Hong Kong China and in Tokyo Japan (see Figure 2). There are plans to add VPN connectivity in Bangalore, India and in Singapore in the near future. Currently there are about 23,000 registered global users using the VPN client. Internet-based broadband VPN has become a popular, widely used productivity-enhancing tool within Cisco.

By migrating to VPN, Cisco IT was able to significantly reduce the per-user costs associated with providing remote access. In addition, Cisco IT was able to significantly reduce staff overhead dedicated to installing and servicing remote access end-user equipment. However, the popularity and ubiquity of Internet-based VPN has multiplied our end-user base by about two and a half times, but our overall costs have increased only marginally. These costs are outlined in detail in the following “Cost Savings” section. In addition, by providing feedback about the product and services, Cisco IT has contributed to the enhancement of the VPN products for all other enterprise customers. We have also captured a few of the lessons we have learned in managing a large deployment of VPN connectivity, and have documented them in the “Lessons Learned” section later in this case study.

Cost Savings

In a direct comparison between the Cisco IT-managed private DSL service and user-managed broadband VPN service, the VPN service provides immediate savings in user service costs and service management costs. The user service costs to provide Cisco managed DSL service were about $100 per employee per month. In comparison, the

cost for each Cisco employee to buy their Internet access now averages about half that (about $50 per month), although that depends significantly on their location and the type of Internet access available in their area (these can include ISDN, DSL, cable, or leased lines). Cisco has created an entitlement policy that requires manager approval to reimburse the VPN monthly charge, of up to US$100 a month. Initial deployments averaged about $60 per employee, but the bulk of Internet access charges have averaged about $50 per employee per month, which is about half the cost that Cisco was charged for the fully managed Rhythms DSL service. So, in a direct comparison between the Cisco IT-managed private DSL service and user-managed broadband VPN service, the VPN service provides immediate savings of about $50, or 50 percent of the total cost, per employee per month.

Service management costs dropped significantly when Cisco IT migrated from the IT-managed DSL service to the user-managed VPN service. Nine of the 10 Cisco IT remote access engineers moved to other jobs within IT, and the remote access group hired two contractors to help support remote access services. This significant reduction in force removed more than $90,000 per month from the IT remote access budget.

In a direct comparison of Cisco IT's remote access costs in migrating almost 10,000 users from private DSL service to user-managed VPN service, Cisco IT saved $496,000 per month, with a ROI of about 6 months (see Table 1).

Table 1. Comparing Costs of 10,000 DSL Users with 10,000 VPN Users

	Clients	Client One-Time Cost	Total One-Time Cost	Client Monthly Cost	Total Monthly Cost
Before migration					
Rhythms DSL service charges					
Remote access IT employee (labor) costs - 10 engineers	9366			$100	$936,600
Totals pre-migration					$120,000
	9366				$1,056,600
Post migration non-VPN					
SBC vendor managed - RLAN					
SBC DSL, VPN (user managed)	228			$110	$25,080
827 Router cost	2833	$180	$509,940	$67	$189,811
827 handling, configuration cost	3061	$180	$550,980		
Circuit installation, project coordination costs	3061	$180	$550,980		
User managed VPN	3061	$180	$550,980		
Remote access IT employee (labor) costs - 1 engineer, 2 consultants	6305	$150	$945,750	$50	$315,250
Totals post-migration					$30,000
	9366		$3,108,630		$560,141
Total monthly cost savings					$496,459
Payback period			6.3	months	

However, the costs of migrating to VPN services late in 2001 were complicated by one significant factor. The earlier managed DSL service was not available to many employees because the Rhythms DSL service had a limited service area. But when we migrated to VPN service using Internet access, which is available to many more employees than the DSL service, the number of users more than doubled from 9300 to more than 23,000 in about a year. Because of this, even though the total cost per user is reduced by half, the total costs to Cisco have increased by about 18 percent. Still, we see this as enabling two-and-one-half times as many users to gain high-speed remote access to improve their productivity for about the same price (see Table 2).

Table 2. Comparing the Costs of 10,000 DSL Users and 23,000 VPN Users

	Clients	Client One-Time Cost	Total One-Time Cost	Client Monthly Cost	Total Monthly Cost
Before migration					
Rhythms DSL service charges	9366			$100	$936,600
Remote access IT employee (labor) costs - 10 engineers					$120,000
Totals pre-migration					$1,056,600
	9366				
Post migration non-VPN					
SBC vendor managed - RLAN	228			$110	$25,080
SBC DSL, VPN (user managed)	2833	$180	$509,940	$67	$189,811
827 Router cost	3061	$180	$550,980		
827 handling, configuration costs	3061	$180	$550,980		
Circuit installation, project coordination costs	3061	$180	$550,980		
User managed - VPN	20000	$150	$3,000,000	$50	$1,000,000
Remote access IT employee (labor) costs - 1 engineer, 2 consultants					$30,000
Totals post-migration	9366		$5,162,880		$1,244,891
Total monthly increased cost					$188,291
Increase in number of users					146%
Increase in cost					18%

LESSONS LEARNED

We expected that the biggest challenge in moving to a user-managed VPN service would be with the user-management portion of the service— users would have problems selecting, installing, and getting repairs to their

service on their own. Cisco IT had always handled all those issues for our users, and we were unsure how successful we would be in handing this responsibility over to end users. As it turned out, users had very few problems selecting their ISP, getting service installed, and managing their own Internet vendors.

The biggest initial source of trouble calls for Cisco remote access has been issues with first-time use. Users now have to set up a VPN tunnel, which requires running the VPN client software application and typing in a login and password each time they connect to the Cisco intranet, about once per day. Getting the Cisco IT approved one-time password requires opening and running another application, SofToken. After getting familiar with the process of running both the VPN client software and the password generating SofToken software, it takes less than 30 seconds, but at first it is difficult. The Cisco IT remote access team created user manuals that explained, step by step, how to do this which helped very much, but not all users were aware of this resource, and many called the internal support group for help.

Another issue for VPN users is setting user expectations about Internet stability, which affects VPN tunnel instability. Short drops in Internet connectivity from the user's ISP would normally not be noticed by an end user of standard Internet connectivity; but this can cause the VPN tunnel to drop, and require the user to go through the process of getting another password and resetting the VPN tunnel again. Although this takes less than a minute, it is something that users were initially not familiar with, and continues to cause some minor user irritation. Some users report that their VPN tunnel remains up for weeks or months without fail, and others report having to restart their VPN tunnel several times in a week.

Issues related to maximum transmission unit (MTU) remain some of the most frequent technical problems, but MTU issues have been minimized in the newer Cisco VPN Client release 4.0 which provides a separate virtual adapter for the IPSec interface. "The typical problems include users able to browse but unable to send or receive e-mail messages, especially with attachments, unable to access NT shares, etc.," says Sonny Parmar, GTRC analyst. The early workaround required the user to change the MTU using the "set MTU" option in previous versions of the client. With clients using DSL with Point to Point Protocol over Ethernet (PPPoE), the workaround was more difficult, as adjusting the MTU on the PPPoE client takes more time. Adding a separate virtual adapter to the Cisco VPN Client in version 4.0 resolves this issue

A second early technical issue that caused some concern was with upgrading the VPN client. Some versions of the client installer software developed by Cisco IT left parts of the Windows registry unchanged, and these changes needed to be removed or changed manually. Users were guided through this process by support staff, but it required a good deal of time from the IT support staff. All registry changes were automated in the integrated Microsoft installers in version 3.6 and all successive versions.

A third technical issue of historic note was that some of the ISPs including AT&T cable service required their users to change their computer name when connecting with the ISP network. After changing the computer name the users found they were no longer part of the Cisco IT Active Directory domain, and so they were locked out of the computer and unable to connect through VPN or pass traffic after connection. Cisco IT recommended that employees use NetSwitcher, a software application that creates separate system profiles for the computer to handle this problem. NetSwitcher is available to employees for download from SoftTracker and is supported by the GTRC. (AT&T cable Internet access service has changed its policy and no longer requires a computer name change.)

One last technical issue arose when Cisco IT arranged with the local telephone company (SBC) to deliver DSL-based VPN access to some of our first VPN users. Cisco IT insisted on our employees using Cisco 827 ADSL routers for DSL access, and SBC did not support Cisco 827 ADSL routers. Cisco IT spent months working with SBC to certify the Cisco 827 Router, and to train their support staff in handling Cisco 827 Router issues as part of SBC's regular support process.

Other lessons learned include the following:

Minimize client versions supported—We found that we needed to minimize the number of versions of client software supported at any given point of time. This would greatly assist in support and troubleshooting. Each new client release contained several features that differed from previous versions, and training support staff on each version's feature set complicated the troubleshooting process.

Do thorough client version testing—We found it critical to thoroughly test a new software client version by means of close-looped pilots and trials (trials with at least 100 end users of varying degrees of expertise, with a set time period and end date) before rolling it out to production. This allowed Cisco IT to identify bugs and workarounds, to generate user training material and Q&As, and to help train support staff on common problems and workarounds.

Maximize tunnel duration—When we first started VPN deployment, our Information Security group established a policy of limiting the amount of time that a tunnel could remain up. They set a policy of dropping a tunnel if the tunnel was idle for more than 30 minutes, and also of dropping all tunnels after a maximum connect time of 24 hours. This minimized the risk that an illegitimate user could use a secure tunnel when the legitimate user was away from their PC for any length of time. However, we immediately ran into user problems with this policy. Users were unhappy having to restart VPN tunnels because they had stepped away from their PC, and they felt that their homes or hotel rooms were sufficiently secure against illegitimate users. More importantly, many application designers and software engineers working from home would set up jobs to run over a long period of time, and had been coming back to find that their session had been terminated before the job had completed, requiring them to start over again and wasting a good deal of time. Cisco IT finally decided that the productivity gains of allowing tunnels to be maintained without time limits was worth the increased security risk, and we removed the tunnel duration limitation.

Simplify the architecture—We found it helpful to simplify the headend Cisco VPN 3060 Concentrator network design wherever possible. For example, Cisco IT avoided using the Reverse Route Injection feature of the Cisco 3060 Concentrator, because it is not supported with EIGRP, our chosen network routing protocol. Instead we dedicated a separate IP address pool (RFC 1918 address space) for each concentrator, and set up a static route from the access gateway for that address pool to the appropriate concentrator.

Work globally—We also found it helpful to work closely with the various global teams so that when local issues are identified those issues, and their solutions, can be shared with the global teams. This allowed us to benefit from the experience of a much larger and wider audience, and increased our ability to find better workarounds and better support strategies.

NEXT STEPS

Many new directions for interesting services are possible with the current VPN solution that would not have been possible with other remote access service options. Our initial investment in the flexible VPN technology allows Cisco IT to make changes to the architecture relatively easily, and to combine simple remote access with various other technologies like voice, video, and wireless, and eventually to eliminate the VPN software client as well. Cisco IT is working on improving the current remote access service by expanding the number of VPN gateways, providing faster upgrades, and making use of better encryption and data compression software. We are also working on enhancing the current service by supporting hardware VPN clients for home access, supporting voice and video services across the Internet VPN, providing extranet VPN connectivity, increasing mobility by supporting wireless connections for PCs and PDAs, and looking to move beyond a VPN software client by supporting SSL-supported browsers for VPN connections.

Expansion of service—Cisco IT is planning to deploy VPN headend concentrators at several new locations. There are many locations worldwide where Cisco employees must connect to a VPN gateway location, which is inconveniently far from them, reducing overall performance of their VPN connection. Although Cisco IT has a policy of trying to minimize the number of Internet access points on the network to reduce security risks, we also try to balance that concern with our user's needs for more convenience and better remote access performance. Locations

currently being considered for possible VPN gateway service are, Singapore, Bangalore India, and Beijing China. Cisco IT will continue to listen to our end users in determining where we need to build additional VPN gateways.

Faster upgrades—Going forward with Cisco VPN Client Version 3.6, IT will be using the Microsoft installer version of the software, which will significantly reduce the time involved in quality assurance testing and rollout of a new version of VPN software. Previous versions required Cisco IT to write our own batch installers and test them before upgrading to a new VPN client version, which reduced our ability to deploy new upgrades quickly.

Better encryption—Cisco VPN Client Version 3.6 also supports the Advanced Encryption Standard (AES), which Cisco IT and Cisco Information Security are evaluating as an alternative to 3DES encryption. The AES algorithm provides for multiple levels of encryption based on the requirements of the user group, and will allow a new level of both security strength and speed.

Data compression—Cisco IT is evaluating several compression techniques for providing better throughput with lower-bandwidth VPN service. Users who cannot find high bandwidth Internet connectivity must use dialup or rate limited DSL connections, and find their lower throughput to be a frustrating limit to their productivity. We are looking at ways of integrating software compression with the VPN client to support throughput improvements for these users. At present one form of compression has been turned on for dial up users using VPN to connect to the corporate network.

Hardware client for home office—Home office users are currently trialing various forms of hardware VPN clients, including the Cisco VPN 3002 Hardware Client and the Cisco 831 Ethernet Broadband Router. This allows them to link multiple IP endpoints across a single VPN tunnel, and provides a functional and productive home office environment. These home office pilot users are connecting their Cisco IP phones, PCs, servers, and video cameras to Cisco across a single secure tunnel established by the router or hardware client. Recent testing of quality of service support from Cisco routers supporting home access has proved useful in supporting better quality voice and video for end users.

Voice and video over VPN—Cisco IT is piloting voice and video over the broadband VPN link from home offices, customer offices, and from hotels. We have been investigating the use of Cisco IP phones with hardware clients, and the use of the Cisco IP SoftPhone application running on the user's PC to provide voice over the PC-based VPN connection. SoftPhone support is currently not available across all theaters, but it is supported by pilots and showcased in some of the theaters.

Extranet connections—Remote access VPN is being evaluated to provide secure connectivity to extranet partners in small sites. Cisco IT is planning to use the Group Lock feature of the Cisco VPN 3060 Concentrator, which allows Cisco IT to create multiple VPNs and ensures that each user is limited to connecting only to their appropriate VPN. Cisco IT will build extranet VPNs, and this provides each partner group with a certain limited set of endpoints within the Cisco intranet that they are able to reach, thus enhancing the security of Cisco proprietary information.

Wireless vendor support—Cisco IT is evaluating wireless VPN technology to provide "anytime and anywhere" access to the highly mobile sales and marketing forces. Pilots are being conducted with various service providers who support broadband mobile transport technologies including GPRS and CDMA 2000. Users describe being able to work from trains or in a car (as a passenger) while remaining continually connected to the intranet and accomplishing meaningful work. In addition, Cisco IT is working with various wireless hot spot vendors like iPass to provide wireless connectivity from several hotels, airports, coffee shops, and restaurants worldwide, greatly improving employee mobility.

PDA support—Cisco IT is investigating some personal digital assistant (PDA) software packages that support IPSec standards for use as VPN client endpoints. PDAs with wireless support will allow Cisco employees a greater degree of mobility than is available today.

SSL support—Cisco IT will be evaluating the Secure Sockets Layer (SSL)-based VPN client functions that will be supported later this year. Cisco IT wants to be able to provide secure and authenticated VPN connectivity to all Cisco employees who have access to a browser supporting SSL, without requiring the installation or use of a separate VPN client.

Contacts

For more information about remote access VPN deployment, start a conversation with the IT subject matter experts in Cisco@Work Security forum at:

http://iforums.cisco.com/iforum/servlet/SCom?page=scom&folderID=caw&CommCmd=MB?cmd=display_messages&mode=new&location=.1dce1eb3

(NOTE: This will be removed for the PDF document that will be given to external customers; it will be retained in the html that will appear on the internal web site.)

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.**