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

A Cisco on Cisco Case Study: Inside Cisco IT
Overview

- **Challenge**
  
  In 2001 Cisco’s DSL provider filed bankruptcy. Cisco® IT had to migrate 9000 remote access users to a new service within one month.

- **Solution**
  
  Migrate from the service provider managed service model to a “user” managed model based on a software VPN client.

- **Results**
  
  Today users can access the corporate network from any location that has a public Internet connection. Usage has almost tripled.
Next Steps

Cisco IT is 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.
History - Incomplete Coverage – 1999

- With the growth of the Internet and the advent of broadband access available to homes, IT started working with various service providers and multisystem operators (MSOs) to provide broadband access to homes.

- Biggest challenge: Multiple vendors, incomplete coverage

  Our goal was to provide the best service to the most employees at a reasonable cost to Cisco®.
Rhythms NetConnections was selected 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.
Challenge - Remote Access Crisis

- August 2001: Rhythms Net Connections filed for bankruptcy; more than 9000 employees depended on the DSL service Rhythms provided.
  
  The remote access team faced migrating 9000 users in a single month.

- IT knew from experience that migrating to other standard remote access services like ISDN or another managed DSL service would be costly, and take more than 10 times their available staff.
Solution - VPN Solution

- The remote access crisis forced IT to consider other options, and to accelerate our migration to a software client VPN solution

- IT reviewed different options and selected a new model
  
  User-managed services based on a software client VPN
  
  User would be responsible for providing their own best-available connectivity to the Internet
  
  Cisco® would reimburse remote access charges as needed
  
  Cisco IT would provide and support VPN connectivity from the Internet gateway to the Cisco corporate network
Solution - Business Issues with Remote Access

- Client productivity
  High-speed remote access means that employees can perform almost all work functions from home or while traveling. For many employees this translates to an additional 10 to 40 percent productivity per day.

- Client satisfaction
  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.

  In 2001 Cisco® had 9000 DSL users and in 2003 Cisco had more than 23,000 VPN users.
Solution - Business Issues with Remote Access

- **Globalization**
  
  A global company must enable its global employees to work together effectively. Due to differing time zones, some employees have to host or attend conference calls at all times of the day. The VPN service connects employees at high speeds to the corporate intranet, letting them work from any location and at any time, much more conveniently.

- **Flexibility**

  Remote access provides added flexibility during a crisis and also for everyday activities.

- **Manual support**

  Because almost all Cisco employees provide their own broadband VPN remote access service, we do not do installations or service calls and we do not do bill reconciliation.
Security

Now that we have migrated to an Internet VPN access service, we do not have to close their Internet service account; the ex-employee can choose to do it if they want. We only have to close an ex-employee's access from the Cisco authentication, authorization, and accounting (AAA) server, which we can do in less than 24 hours, to keep them from accessing the Cisco internal website.
Solution-Business Issues with Remote Access (Contd.)

- Cost

  The cost to provide user-managed VPN service is about half the cost to provide Cisco IT-managed high-speed access service.

  The cost to each Cisco employee for Internet access depends on their location and the type of Internet access available in their area (access types can include ISDN, DSL, cable, or leased lines), but it still remains about half the cost of DSL access provided by Cisco.

  Users select the best-possible service at their locations, providing more flexibility than an IT-selected service could offer.

  Cisco reimburses employees, when possible, up to a preset limit.
Solution-Network Architecture and Design
Results - VPN Concentrator Locations
Results - Summary

- Internet-based broadband VPN has become a popular, widely used productivity-enhancing tool within Cisco®

Today users can access the corporate network from any location that has a public Internet connection. Currently, about 23,000 registered users worldwide use the VPN client.

- Cost savings

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.
Next Steps - Summary

- **Expansion of service**
  
  Locations currently being considered for VPN gateway service are Singapore; Bangalore, India; and Beijing, China

- **Faster upgrades**
  
  Going forward with Cisco® VPN Client Version 3.6, IT will use 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.
Next Steps – Summary (Contd.)

- **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.

- **Data compression**
  
  Cisco IT is evaluating several compression techniques for providing better throughput with lower-bandwidth VPN service.
Next Steps - Summary

- Hardware client for home office
  Home office users are trying various forms of hardware VPN clients, including the Cisco® 831 Ethernet Broadband Router.

- 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.

- 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.
Next Steps - Summary

- **Wireless vendor support**
  Cisco® IT is evaluating wireless VPN technology to provide "anytime and anywhere" access to the highly mobile sales and marketing employees.

- **PDA support**
  Cisco IT is investigating personal digital assistant (PDA) software packages that support IP Security standards for use as VPN client endpoints. PDAs with wireless support will allow Cisco employees a greater degree of mobility than is available today.
Next Steps - Summary

- SSL support

Cisco IT will evaluate 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.
A Complete VPN Solution

- Offer a complete VPN solution, and meet the needs of your business customers today