Top 5 Considerations for Cisco Unified Communications Deployments for Telecommuters

Organizations are seeking to take full advantage of their unified communications deployments by extending these services to remote locations and to telecommuters. Working from home provides benefits to both employees and businesses, including flexible working, better work-life balance for employees, and helping to lower the carbon footprint of the organization. The following are some things to consider when making decisions about extending a unified communications system to support telecommuting.

1. Remote Multidevice Support

In simplistic unified-communications-based telecommuter deployments, solutions such as phone proxies can be applied to enable Cisco IP phones to securely connect across a public infrastructure and integrate with the enterprise unified communications system. However, in fixed-site remote telecommuter locations, many devices can benefit from a remote VPN device that can secure all traffic. Network-connected faxes, printers, PCs, and phones do not all have VPN capability; a remote router with VPN capability provides a single, manageable platform for providing confidential communication for all devices at a remote site.

2. Simplified User Experience

Executive users of remote unified communications services often demand a simplified user experience when they telecommute. Essentially, they want to have the same user experience as when they are in the corporate office; for example, they might want to be able to connect a device into the remote network without needing perform additional administrative tasks. As unified communications extends beyond the phone to include presence, instant messaging, and other data-oriented applications, a secure remote-access device can remove the user's administrative burden.

3. Remote Site Protection and Control

When extending unified communications solutions to telecommuter environments, organizations may need to add security to remote devices in order to comply with certain regulations and requirements. By using a remote router that can provide firewall, intrusion prevention, and secure communications through VPN functions, organizations can apply security controls that are centrally managed, easing the burden of security from the end user. The Cisco Enterprise Class Teleworker (ECT) solution provides a proven architectural framework for provisioning and managing remote device teleworker solutions.

4. Quality of Service

A challenge of telecommuting services is assuring the quality of the services the user can access. For data applications, quality of service requirements can use a lower-cost network infrastructure such as the Internet; securing through an IPsec and SSL VPN user service is acceptable. Voice traffic, however, is sensitive to delay and jitter; poor quality of service capabilities can lead to unusable voice services. Additional challenges when providing telecommuting services over an

infrastructure such as the Internet include the traffic on the link from the end user's home to the service provider. In what is typically a multidevice deployment, end-user applications such as e-mail or Web browsing can result in data applications swamping or interfering with smooth delivery of voice traffic. By using a secure remote network device, organizations can apply intelligent quality of service and queuing mechanisms to reduce the impact of data applications on voice services.

5. Troubleshooting and Diagnostics

A common concern in many organizations is the cost of managing remote telecommuter environments; particularly, the cost of deploying and managing equipment at the remote site. It is important to remember that remote devices can help IT teams troubleshoot and diagnose issues in telecommuter deployments more quickly and easily. Many telecommuters are not trained to troubleshoot and resolve IT issues on their home network. When taking into consideration the challenges associated with resolving remote issues on systems that may or may not be corporate-owned, organizations will often find that the cost of support can be more significant than the cost of the remote network security equipment itself.

References

- Cisco IOS Security Services: http://www.cisco.com/go/iossecurity
- Cisco Enterprise Class Teleworker (ECT) solution: http://www.cisco.com/go/ect

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.

Printed in USA C96-458661-00 03/08

