Working Green

Bottom-line benefits
of telecommuting and secure remote access

White paper
February 2008

Tim Clark, Partner
The FactPoint Group
349 First Street
Los Altos, CA   94022
(650) 233 1748
tclark@factpoint.com

Introduction

Growing public concern about global warming and other environmental issues is spilling over into the business world, where companies are increasingly looking to make their operations more "green" by minimizing their environmental impact. The reasons range from scarcity of resources to the boost to corporate image to potential cost savings by using more environmentally sensitive activities.

This white paper explores telecommuting and addresses environmental benefits, advantages to employers, advantages to employees, technology requirements and issues to address.

Business strategies to go Green

- Promote telecommuting with secure remote access technology.
- Redesign products to use more environmentally friendly materials and require less power to reduce their carbon footprint.
- Reduce consumption of electric power in company facilities, particularly for data centers and always-on desktop computers.
- Buy green or recyclable/reusable office supplies and recycle to divert waste from landfills.
- Encourage carpools, public transit and bicycling for commuting workers or even subsidize employee purchases of hybrid vehicles, as Google does.
- Convert truck fleets to biofuels, as grocery chain Safeway has, reducing carbon emissions by 75 million pounds annually—the equivalent of taking 7,500 cars off roads.

User cases for secure remote access—telecommuting and beyond

Telecommuting, sometimes called telework, is the practice of allowing employees to work from home. It's hardly a new idea, but telecommuting is gaining new attention because of high gasoline prices, increased broadband Internet access from homes and a growing understanding that excessive use of personal vehicles contributes to air pollution and global warming. Advocates note that workers who telecommute just one day per week cut their commute-related emissions by 20%.

How big an impact could telecommuting have? In a 1996 review of transportation studies, D.L. Greene concluded that telecommuting could reduce vehicle travel by up to 3.4% of total vehicle miles. That made telecommuting the third most effective transportation control measure after congestion pricing (5.7%) and land-use planning (5.2%). Unlike land-use or congestion pricing, companies and individuals can implement telecommuting on their own.

In a twist on telecommuting, some companies maintain popular satellite centers where workers can work near their homes instead at home or their distant office. In the United Kingdom, satellite sites are called "telecottages" and often are run by entrepreneurs for multiple employers.

For telecommuting, a critical requirement is secure remote access to enterprise applications and data. Without secure access, telecommuters are cut off from the tools needed to do their jobs effectively, or the employer opens itself to dangerous security breaches.

Telecommuting is not the only scenario for secure remote access. "We have many locations around the world with multiple remote contributors. These road warriors—sales people, systems engineers and developers—all benefit from secure remote access," said SonicWALL customer Richard Grey of Cyclades, now part of Avocent.

Remote access scenarios

Telecommuting: Knowledge workers.
Disaster recovery: Business continuity a key requirement.
Road warriors: Sales, systems engineers, developers.
Partners: Suppliers, channel, outside vendors.
Business services: Client site work for consultants, accountants.
Health care: Patient files, distant transcribers, tele-radiology.

Companies that work closely with partners or suppliers may let outsiders log in to see specific relevant data on corporate systems. "Factories need to review designs to freelance designers working with our internal teams," said Tammy Barrett of clothing manufacturer Patagonia, another SonicWALL customer

At Witt Mares, a Virginia accounting and business consulting firm that uses SonicWALL for secure remote access, tax specialists frequently work at client offices. "We use remote computing to bridge the gap between our offices and where our clients need us to be," said Brent Reed, senior network engineer for Witt Mares. In the past, when remote staffers need specific files or information on Witt Mares' network, files would be faxed, e-mailed or hand-delivered to client locations. With secure remote access, the firm no longer must dedicate staff to support remote workers.

Accounting work involves confidentiality, as do health care requirements (HIPAA) for securing patient medical records. Remote access in health care may involve overseas medical transcribers or physicians seeing hospital patients whose records are at the medical office. Virginia-based Potomac Hospital uses SonicWALL for a virtual private network (VPN) for remote doctors and services providers, including an Australian vendor that uses the VPN to read x-rays. The hospital has more than 250 people working remotely, including 60 individuals on the VPN at any one time.

"Our hospital security system ensures the integrity of our network and the security of our patients' information, while allowing our medical professionals to provide quality patient care from wherever they are working," said Tony Davis, Potomac's network systems manager. Adds another SonicWALL health-care customer, Tina D'Amico of County Obstetrics and Gynecology in Connecticut: "We now have a secure, HIPAA-compliant solution that allows my physicians to access the files they need from anywhere, at any time, from the labor and delivery room to their home office."

Companies already using secure remote access can easily add a telecommuting component with the same VPN infrastructure.

Green benefits of telecommuting

Fundamentally, telecommuting with secure remote access allows companies and their employees to reduce their carbon footprint in two direct ways: First, by reducing the use of petroleum products to power their commute vehicles, and, second, by reducing the environmental costs (and demand) for manufacturing additional automobiles.

Employers strike Green in telework

IBM

- In 2005, the U.S. work-at-home program involved 20,000-plus employees, saving more than 5 million gallons of fuel and avoiding more than 50,000 tons of CO_2 emissions.
- More than one-third of IBM's global workforce (100,000-plus employees) participates in work-from-home or mobile employee programs.

Hewlett-Packard

- 70% of HP's employees telecommute at least occasionally.
- Nearly 13,000 employees work exclusively from home offices, about 10,400 in North America.
- In 2006, full-time telework saved almost 2.5 million round drips, avoided 85 million miles of road travel and almost 28,000 tons of CO_2 emissions

CH2M HILL

- Engineering firm allows full-time teleworking for employees whose jobs permit.

Intel

- In 2003, 44 percent of Intel's 48,600-plus U.S.-based employees were able to take advantage of telecommute options.

LexisNexis

- Started telecommuting pilot in 1995, saving the company $6 million in the first year.
- Program continues to run profitably.

Reducing solo commutes also cuts air pollution, which carries the additional benefit of improving the population's health, especially for people with respiratory ailments. These benefits accrue to the telecommuters, the earth and its billions of residents.

In addition, companies can claim another set of benefits by supporting telecommuting. Most significantly, these companies may cut their real estate costs by not providing a full-time cubicle or workspace for every knowledge worker on the payroll. If employees work from home, employers also consume fewer resources (land, building materials, energy) for office buildings typically used only a third of the day.

In other cases, telecommuting can boost regulatory compliance. Stanford University, for example, is required by local authorities to cap car trips onto campus during peak commute period at the levels of 2001—despite a steadily growing workforce. Stanford promotes a wide range of commute alternatives. In Delaware, the 275 employees in AstraZeneca's telework programs help the company meet a state traffic mandate.

Company brands also benefit from a “green” reputation, which explains why 269 worksites covering 629,000 employees of Fortune 500 companies have applied for and earned a “Best Workplaces for Commuters^{SM}” designation, established by the U.S. Department of Transportation and Environmental Protection Agency to recognize employers that address impacts of driving-alone commutes.

Telecommuting also creates environmental and social benefits that spread beyond the employer and its employees. Telecommuting also reduces traffic congestion. Fewer cars on the road mean over time lower public infrastructure costs for roads and bridges, also lowering the consumption of raw materials to build that infrastructure.

Other business benefits of secure remote access

Perhaps the biggest additional benefit of providing secure remote access for telecommuting is the boost to the company’s disaster recovery efforts. When bad weather, a power outage or natural disaster hit an area, typically it does more than knock out a data center. Switching over to a back-up data center may prove to be the easy part if employees cannot get to the office to do the work.

In such business continuity situations, allowing employees to work securely from home with access to their usual data and application becomes a critical element of the recovery. Radiology Ltd., a SonicWALL customer in Tucson, Arizona, that provides diagnostic imaging services, installed a VPN to send images but it also doubles as part of its disaster recovery infrastructure, particularly for branch offices. In the event of a business disruption, employees simply go to a secure portal to access all needed resources.

Other benefits of secure remote access

- **Disaster recovery**
- **Utilize distant suppliers**
- **Reduce office costs**
- **Reduce real estate costs**
- **Accommodate disabilities**

In addition, a distributed workforce also reduces the company’s vulnerability to outages, which generally have a geographic focus.

Likewise, a distributed workforce can reduce office operational costs (and resource consumption) for power, cooling, desktop computers, furniture, phone land lines and other standard office requirements for knowledge workers. As mentioned, avoiding real estate costs can comprise a substantial part of a telecommuting use case. In 2005, Sun Microsystems reported saving $255 million in real estate costs over four years by eliminating or avoiding the need for 7,700 cubicles and workstations.

In addition, the U.S. Equal Employment Opportunity Commissions states that employers can accommodate disabled employees, as required by the Americans with Disabilities Act, by allowing them to work from home.

Employee-related benefits of telecommuting

In early 2008, FORTUNE magazine reported that 84 of its 100 “Best places to work” offered telecommuting, up from 18 in 1997. Clearly employees like the telecommuting option, but why should employers?

The phrase “Happier employees are more productive” summarizes the reasons, but the specifics are important. Companies with telecommuting programs tout increased employee well-being, greater flexibility, better work-life balance and more employee control of their time. Sun Microsystems found workers save 90 minutes a day in drive time and hassles using satellite facilities. Anecdotal evidence suggests lower absenteeism and use of paid sick time, in part because telecommuting reduces employee stress and fatigue.

How telecommuting pleases workers…

- **Less stress**
- **More flexibility**
- **Work-life balance**
- **Control of time**
- **Lower commute costs**
- **More time at home**

…and employers too

- **Higher productivity**
- **Lower absenteeism**
- **Better job satisfaction**
- **Higher retention rates**
- **Lower training costs**
- **Easier recruitment**

Beneath those productivity benefits is the reality that telecommuting employees spend less time commuting and more time at home, which many see as a benefit itself. Employees’ commute costs are also lower. In addition, telecommuting produces higher job satisfaction and employee retention, valuable themselves but also reducing training costs because of lower employee turnover.

Companies that offer telecommuting also benefit in recruiting new employees, because telecommuting is seen as positive by potential employees. For two-career families, telecommuting means one partner’s relocation need not force the other to switch jobs too, adding both geographic and professional flexibility.

Technology requirements for telecommuting

The core requirement for telecommuting is the ability to offer secure remote access to telecommuting employees, giving them authenticated access to business data and applications that each specific employee is authorized to use, just as in the office. Secure authentication technology is a prerequisite, and VPNs are one way companies can provide such secure access.

The type of VPN is important. Companies don’t want set-up and management headaches; they want technology that is easy to deploy, use and manage. It should be quickly scalable, especially if the telecommuting solution doubles as a disaster recovery technology. That means avoiding “pay per connection” charges that can run up the tab if telecommuting catches fire.

The VPN technology must ensure compliance to data security policies and regulatory mandates that apply to that specific company and industry. The VPN solution should offer granular access to all corporate applications—different telecommuters will have different needs and authorization to access, so the remote access solution must have the flexibility to deal case by case. Companies want the highest level of security that is practical given the other requirements.

The Clean VPN: Securing the perimeterless network

The communications landscape is rapidly evolving. The rise of VoIP, proliferating Internet-connected devices, increasing use of real-time applications and the growing savvy of online criminals challenge IT departments that offer secure remote access.

How to respond? Forward-thinking IT departments are shifting their thinking to consider all end points—whether inside or outside the firewall, within or beyond IT's control—as potentially "dirty" (insecure). The network perimeter gradually disappears, leaving the corporate data center and its applications facing a mass of insecure endpoints. With a perimeterless network, all communications must be secured as they flow through the network.

Requirements go beyond simply authenticating the identity of users. The user's location, access device and network link also affect the security of the connection. The perimeterless network requires the Clean VPN. Because network security threats can enter at multiple points, the Clean VPN addresses five critical questions:

Scenarios for Clean VPNs

- An employee's home computer doesn't have up-to-date antivirus software, so a virus could pass through to the corporate network.
- A telecommuter logs on from a Starbucks store's wireless connection to check email. That connection's security is uncertain at best.
- At an airport, an employee logs in through an iPhone or Blackberry device. The Clean VPN may limit which applications the user can access from that device.
- A company's consultants or temporary employees must be authenticated and secured, even when they sign on inside a corporate facility.

1. Who is the user? Based on strong authentication, determine identity.
2. What's on the end point? Based on policies for device type or device software, allow the appropriate level of access.
3. How safe is the combination of user, device and location? Employee connecting on her own laptop from Starbucks may get different access than the same employee logging in from home on company-issued desktop.
4. How secure is the traffic? Require real-time inspection of network packets.
5. What resources is the user seeking? Grant access based on policy.
6.

For the Clean VPN, no longer is a standalone SSL VPN appliance sufficient to secure connections based on these five questions. The Clean VPN starts with secure remote access, then adds other protections through Unified Threat Management (UTM) devices that bundle multiple security applications on a single appliance.

Challenges in telecommuting

The telecommuting agreement

Many organizations create formal telecommuting pacts that outline terms, guidelines and expectations for telecommuter. It should address:

- **Work schedules** and timesheets.
- **Hardware requirements**: (computer, phone, office furniture, power surge protectors, etc.) in the home work space.
- **Software**: Antivirus, email, security and compatible versions of productivity applications.
- **Communication, collaboration**: Broadband Internet access, phone, teleconference, corporate network access, fax, instant messaging, voice over IP (VoIP), Web conferencing, etc.
- **Wireless home network** security
- **Access to IT help desk** for computer issues.
- **Policy on phone** expenses and forwarding calls.
- **Confidentiality**: Rules for accessing confidential material and for sharing employer data with non-employees.
- Attending **in-office meetings**.
- Rules for **home office meetings**.
- **Office supplies**: Some employers provide office supplies but won‘t reimburse out-of-pocket costs.
- **Evaluation** of the telecommuting arrangement, both initial and then periodically long-term.

Not every job or every employee is a good candidate for telecommuting. Employees, managers and the company itself each must address challenges inherent in having employees working outside the office.

For employees, telecommuting may increase their isolation from colleagues, reduce their visibility from managers and make access to support services more difficult. It also may increase at-home expenses and reduce living space in the home. Telecommuting also may limit access to training programs, although online training can address that issue.

Telecommuting need not be on an every-day schedule. Have the telecommuter work in the office some days address issues such as missing spontaneous meetings in the hallway.

For managers, the biggest challenge may be managing unseen employees, which requires different procedures and management style. Indeed, supervisors are sometimes the biggest barrier to telework success. LexisNexis trains managers of telecommuters to direct teams that are not physically present.

The role of support staff in assisting telecommuters may also be problematic. On days telecommuters work remotely, they made need on-site help for some activities—faxing paper documents not available in electronic form, for example.

For companies, barriers to adoption may include unexpected operating costs, legal considerations, quality programs and data security. Legal issues include safety (the employer may still be responsible for job-related injuries even in an employee's home), labor laws (on overtime pay and advance approvals of overtime) and collective

The greening of SonicWALL

SonicWALL's VPN appliances enable secure remote access for telecommuting, with the environmental benefits outlined in this paper.

SonicWALL also complies with European Union mandates on electronic waste management (WEEE) and restricting hazardous material in electronic equipment (RoHS).

In addition, SonicWALL bakes power efficiency into its product line:

- **Integrated**: By including multiple functions (firewall, antivirus, intrusion protection anti-spam, spyware, URL filtering and VPN concentration) in a single Unified Threat Management appliance, SonicWALL reduces power requirements over a single device for each function.
- **Multicore**: Using multi-core processors (as many as 16 in NSA E7500) increases the through-put per kilowatt beyond the ratios of competitors.
- **Space**: Integrated SonicWALL appliances need less rack space in data centers.
- **Cooling**: Integrated SonicWALL appliances produce less heat, cutting cooling costs.
- **Battery life**: In an electrical outage, a power-efficient SonicWALL device runs longer on back-up power, putting less of a load on generators.

bargaining agreements (such as shift-based pay differentials). For unionized employees, employers may want to discuss telecommuting policies with the relevant union before implementing or revising rules.

Telecommuting seems to work best for certain types of work. The University of Oregon identifies accountants, auditors, data entry operators, financial analysts, programmers, systems analysts, researchers, writers and editors as among the many job titles that may adapt well to telecommuting.

Not every employee is well suited for telecommuting. Chances of success are highest when the employee is mature, self-disciplined and capable of working with little on-site supervision. Consistently positive performance evaluations are a good indicator of likely success. Strong candidates are dependable, well organized with good time-management skills, and have the required computer expertise to make telecommuting successful.

To make telecommuting work, the employee and supervisor need a level of trust and a commitment to ongoing communications. Otherwise, the distance between supervisor and employee may strain the working relationship. Managing from a distance takes a new set of skills, and some companies with telecommuting programs are implementing training programs for managers overseeing telecommuters.

Telecommuting resources

Telecommuting, University of Oregon human resources department, which has overseen campus telecommuting since 1999. http://hr.uoregon.edu/policy/telecommuting.html. Also see the university's Telecommuting Policy (http://policies.uoregon.edu/ch3x2.html) and a Telecommuting Agreement form (http://hr.uoregon.edu/policy/tele-agree.pdf).

The Teleworking Handbook, 352 pages, 4th Edition, published by The Telework Association (http://www.telework.org.uk/), bills itself as the most comprehensive guide for teleworkers and organizations introducing remote working schemes.

TransportEnergy Best Practices: A guide to teleworking: How to increase your business efficiency. 44 pages, Department of Transport (United Kingdom), http://www.energysavingtrust.org.uk/uploads/documents/fleet/TE192_Teleworking_guide_final_version.pdf

About SonicWALL

SonicWALL is committed to improving the performance and productivity of businesses of all sizes by engineering the cost and complexity out of running a secure network. For more information, visit the company web site at http://www.sonicwall.com/. Secure remote access information is available at http://www.sonicwall.com/us/products/Secure_Remote_Access.html.

About The FactPoint Group

The FactPoint Group (www.factpoint.com) is a Silicon Valley-based market research, publishing and consulting firm specializing in the early adoption of new technologies. The FactPoint Group has been producing world class research, analysis, and consulting since 1993 and continues to help its clients sell and use new technology solutions. FactPoint partner Tim Clark was, until 1999, a senior editor with CNET News.com, where he covered Internet security. Clark authored two white papers on secure remote access for Aventail, which SonicWALL acquired in 2007. He has telecommuted since 1993.