



Key Steps to a Secure Remote Workforce

Telecommuting benefits the employee and the company, the community and the environment. With the right security measures in place, there's no need to delay in creating a remote worker policy that's right for your organization.

CONTENTS

Abstract	2
Offices can become unusable	2
Remote worker access concerns	2
Step one: setting policy	3
Step two: maintain and communicate policies	3
Step three: create a secure telecommuting framework	3
Step four: a layered approach	5
Step five: securing the home	5
Step six: data backup and recovery	5
Conclusion	6

Abstract

The workplace has undergone fundamental changes over the past decade. No longer is the corporation housed within physical walls; it now transcends those buildings, even extending beyond distant geographic borders. The corporate network too, expands far beyond the corporate perimeter to provide access to partners, clients, suppliers, and traveling workers. But the institution that has brought about the greatest change and controversy in the workplace is that of telecommuting.

Telecommuting has become a way of life. Its growing acceptance is driven by many factors including initiatives to reduce pollution and congestion, the soaring cost of office space, and the challenges of communicating across international time zones. State and federal government offices have become the most enthusiastic proponents of teleworking, and most federal agencies are now required to have teleworking programs available to qualified employees. Private corporations, while not under legislative mandate to do so, often find that they too must develop remote worker programs in order to retain quality employees.

Even as a morale-booster, telecommuting has a great deal to offer by allowing workers a more flexible lifestyle. It's a definite attraction for companies based in high-priced urban areas where the cost of living is scaring the workforce away to a longer, more stressful commute. And the high cost of gas doesn't help matters.

Offices Can Become Unusable

Then there's the unexpected. What steps should be taken to prepare against natural, economic or health emergencies such as earthquake, hurricanes, flooding, extreme weather or pandemics like avian flu? A virtual workforce of telecommuters might be the only way of staying in business in the event that the company's facilities are uninhabitable, roads have become impassable, or conditions make a journey to work too dangerous to contemplate.

Remote Worker Access Concerns

Many employers still have reservations about remote working, and chief among their concerns is security. Making the appropriate data available, but only to the right people; securing digital assets and avoiding data leaks; remaining compliant with financial, medical or corporate regulations; managing and supporting a dispersed, non-technical workforce; and maintaining communications despite physical disruption are frequently cited as reasons against instituting more widespread remote worker programs.

The explosion of cheap and widely available broadband access has further revolutionized how people connect to the Internet from home. But this broadband convenience also increases the threat level to the home. As corporations and government agencies step up security to harden their networks, attackers switched their focus to home users, who tend to be more lax in implementing security. Telecommuters in particular represent attractive targets, because the attacker hopes to find a back door to sensitive corporate data.

Today's technology provides many of the answers to these concerns and others, to enable businesses of any size to create a secure, functional and efficient remote worker network. While creating a telecommuting framework involves more than giving employees laptops and a password, it only takes a few steps to integrate an effective and secure telecommuting program into the workplace. Here's an outline of how to get started.

Step One: Setting a Policy

One of the biggest problems in telecommuting is lack of uniformity. Corporate IT and network guidelines need to be applied equally to remote computers to prevent the possibility of telecommuting workers becoming the weakest link in the network. A common barrier to telecommuting is concern over network security, although this need not be an obstacle. With the correct security policies, procedures and technologies in place, a remote connection can be as secure as one located in company headquarters.

Successful and safe telecommuting starts with creating, implementing and enforcing a telecommuting policy. This policy needs to include elements that are both behavioral and technical.

Key Policy Considerations:

- Decide whether employees will be able to use their own personal computers for telecommuting, or whether the company will provide pre-configured, company-owned computers for the telecommuters to take home for dedicated company use. Provide guidance as to how personal PCs should be configured; create rules for version updates and security patches.
- Set boundaries for home network users. If you allow employees to attach their telecommuting computer to their home network, your policy should dictate that file sharing be disabled and that work-related documents are stored onto a removable drive that can be secured separately.
- Create a backup policy for data created by remote workers.
- Provide guidelines to prevent theft or accident. As an example, you'll probably want to make it clear that company laptops or data storage devices may not be left unattended in cars or areas where they can easily be stolen.

Step Two: Maintain and Communicate Policies

- Create a teleworking policy document and have your remote workers sign an agreement to abide by its guidelines.
- Communicate policies clearly and provide regular updates.
- Monitor for breaches of policy. If you don't enforce the rules, they'll fall into disuse.

Step Three: Create a Secure Teleworking Framework

Infonetics Research reports that 92 percent of companies report security as a barrier to implementing VPNs. Other deterrents include concerns about increasing the burden on IT support, bandwidth usage and setting network access controls at appropriate levels.

The connection between the telecommuter's home and the corporate network is perhaps the most sensitive part of the whole environment, and is what scares IT managers the most. VPN, or virtual private network technology will encrypt information and enable it to travel safely between the two locations, but what if that information itself is corrupted, and is carrying malware into the network?

A Dynamically Updated Firewall

Secure the network with a *Unified Threat Management (UTM) firewall* that will scan all network traffic for threats. UTM firewalls are automatically updated with signatures against network threats on a continual basis, maintaining comprehensive protection against worms, viruses, Trojans, spyware, and other malware. Even small organizations should use UTM devices – there is no such thing as a small virus for small business. SonicWALL's UTM network security appliances protect businesses that range from under 10 users up to thousands of employees.

If your firewall does not have *dynamically updated security services*, consider upgrading or adding the capability. A static firewall is only able to secure against threats that existed on the day you installed the appliance, and your network will be vulnerable to new attacks.

Remote Connectivity – IPSec VPN or SSL-VPN?

If you have *in-house IT capabilities*, you may want to opt for IPSec VPN. It routes traffic through your firewall to provide highly secure connectivity, and is a preferred technology for site-to-site communication. IPSec VPN requires IT departments to load a VPN client on all remote users' laptops or home computers. SonicWALL network security appliances are delivered with IPSec VPN user licenses.

If you are looking for *simplicity in securing remote workers* – perhaps you don't have an IT department, or your teleworkers don't always work from the same computer – consider installing an SSL-VPN appliance on your network in conjunction with your firewall. With SSL-VPN there is no need to install client software – all the remote user needs is a standard Web browser, so it's ideal for mobile users as well.

The SonicWALL SSL-VPN Series of appliances integrates easily with the SonicWALL PRO Series of network security appliances, as well as most third-party firewalls. Together the two create a complete solution for perimeter protection and secure remote access.

The Right Data in the Right Hands

You want your remote workers to get access to some network assets, but not necessarily all –an HR employee has different needs from an engineer. SSL VPN technology makes it easy to set very precise network access policies. An SSL-VPN appliance such as the SonicWALL SSL-VPN 200 (for up to 50 employees) or SSL-VPN 2000 (for up to 1,000 employees) enforces a highly granular set of access controls, which allows the administrator to delegate access to very specific and defined resources, so that the right people will have access to the right information. SonicWALL SSL-VPN Series of appliances are highly affordable, so this easy method of enabling remote working is open to businesses of any size, from an enterprise to a start-up.

Proper Configuration

The remote computer's Web browser and operating system can be a source of vulnerability if they are not maintained to the same standard as those within the corporate walls. Make sure each remote worker has access to the latest patches and updates, and that the security settings on the browser are configured appropriately. A global management tool such as the SonicWALL Global Management System (GMS) makes it easier for an IT administrator to manage and monitor a distributed network of teleworkers from a central location.

Step Four: A Layered Approach

Remote workers coming in from the field may be harboring malware on a laptop or USB device. Maintain security behind the network and from department to department by implementing enforced desktop threat prevention, which prevents users from logging into the network if their computer has been infected with viruses or spyware.

Some organizations with heightened confidentiality or security requirements, such as legal, government, finance or medical offices, should consider a network security solution that allows you to sweep for malware as traffic travels within the network and to apply varying security policies depending on the user or workgroup. Firewalls with LAN switching capabilities allow you to secure communications both from external sources and internally from zone to zone. Appliances such as SonicWALL's PRO 1260 Enhanced secure LAN switch can be configured to secure any combination of internal workgroups, public servers, wide area networks and even wireless networks

Step Five: Securing the Home

There are a number of options that create highly secure remote high-speed connections – even for wireless users:

- **Use personal firewall devices for remote high speed connections.** It's a good idea to equip key remote workers (such as network administrators or IT support staff) with a small firewall for their home offices. SonicWALL has ensured that even these small network security appliances deliver dynamically updated unified threat management to protect users from exposure to Internet-delivered attacks.
- **Install IPSec VPN client software on teleworkers'** computers so that they can create a secure tunnel to the company network.
- **Wireless users can be secure too.** Using ordinary wireless routers leaves remote users vulnerable to drive-by hackers, spyware, and other intrusions. A SonicWALL TZ 150 Wireless appliance will provide complete unified threat management protection for up to 10 wired or wireless users for any home network.
- **Maintaining the connection.** Determine which of your key workers in critical functions need network connectivity at all times, and provide them with a small office firewall providing multiple failover options including broadband, dial-up and wireless. The SonicWALL TZ 170 SP Wireless provides all these options, together with comprehensive unified threat management protection to defend against Internet threats such as viruses, spyware, worms and Trojans.

Step Six: Data Backup and Recovery

Whether you save your files to floppy disks, to tape, CD or to a redundant drive, you are undertaking an essential part of business continuity – data backup and recovery. However, mobile media and appliances are vulnerable to accidental loss or physical disaster. Ensuring business continuity by maintaining the availability of important company data is the final piece in the remote worker puzzle.

- **Make it automatic.** To be most effective, backup and recovery should be automatic, reliable and include offsite backup so that a remote worker can retrieve information even if the original device on which it was created has been lost.
- **Make it frequent.** Waiting to backup until a mobile worker reconnects to the office network leaves huge gaps in protection.

- **Recovery is vital.** Backup without the ability to recover is of little use. Today's technology means that companies can now go beyond the limitations of tape archiving to achieve "any point in time" recovery. Disk to disk data protection solutions, like SonicWALL's Continuous Data Protection technology, will allow you to retrieve relevant information quickly after a disaster, as a company, or as an individual working remotely. SonicWALL's Continuous Data Protection technology automatically replicates any new or changed data – in real-time while offsite data storage provides an additional layer of business protection.
- Ensure security and continuity of business data regardless of location. The combination of continuous data protection, offsite data backup, and bare metal recovery (the ability to recover an entire system from scratch, including data, the OS, applications, and all settings and configurations) affords the greatest protection and forms the foundation of a workable disaster plan.

Conclusion

There are dozens of business, economic and social drivers for expanding the remote workforce. While some companies have been reluctant to allow it because of security concerns, there's no question that telecommuting is here to stay. Telecommuting benefits the employee and the company, the community and the environment. With the right security measures in place, there's no need to delay in creating a remote worker policy that's right for your organization.