Securing Teleworkers

Growing security concerns make it more important than ever that IT provide secure access for users working remotely.

An estimated 30 to 50 million Americans "telework" one or more days a week, working from their homes or remote telecommuting facilities instead of going to the office, according to John Edwards, chairman of Telework Coalition, a nonprofit organization enabling virtual mobile and distributed work through education, technology and legislation.

Established reasons for telework include job flexibility to promote employee productivity and retention, along with cost savings through reduced need for office and parking space. The need to provide various services around the clock — financial services, technical support for customers, internal IT support — have also given companies incentive to support telecommuters.

Over the past several years, additional reasons to support telecommuting have gained momentum. Legislation, including the Family and Medical Leave Act, the Americans with Disabilities Act and the Clean Air Act, has added economic and compliance motivations. Recent catastrophic events, ranging from major power outages to Hurricane Katrina, have added business continuity planning as another motive to have telework solutions in place. "In-place telework solutions help organizations be ready for disaster recovery, or for 'social distancing' in case of pandemics," comments Vivian Ganitsky, director of product management at Juniper Networks.

Today's desktop and notebook computers, combined with increasingly available broadband Internet connectivity, have made it easy and affordable for many people to productively work remotely. In addition to e-mail, intranets and file servers, many of today's teleworkers also make regular use of multimedia and collaborative applications like Voice over Internet Protocol (VoIP), videoconferencing, instant messaging, file sharing and collaboration tools.

Increasingly, teleworkers are also using server-based applications running inside the company network or from hosted third-party services. "With server-based computing, supporting remote machines is much easier," notes Chuck Wilsker, president and CEO of the Telework Coalition. "The data is in the company, and settings are easy to replicate."

VPNs: Secure Remote Connectivity

Connections made to the company network from employee homes and other locations via the Internet are deemed inherently unsecure, since there's no way to guarantee nobody is "listening" in. To secure telecommuters' remote connections over the Web, most companies use virtual private networks (VPNs) utilizing either Internet Protocol Security (IPsec) or Secure Sockets Layer (SSL) technologies.

An IPsec VPN is at the network layer, providing a full connection between a remote computer and your company's network. This provides great flexibility, but also means that viruses or other threats on remote computers have full access to the company network. IPsec is most commonly used to connect sites, rather than an individual computer or home office, and requires the teleworker to have IPsec software on his or her computer.

An SSL VPN works at the transport layer of the TCP (Transport Layer Security)/IP protocol stack and is session-oriented. SSL-secured Web sessions are common » for online shopping and banking. Nearly every Web browser today includes SSL features — even the ones on handhelds and Web-capable cell phones.

"SSL VPNs can offer more 'granular' security," says Juniper Networks' Ganitsky. "IT can specify more rules, such as limiting access to specific files, URLs or applications, even what times a user has access to something, versus an IPsec VPN's full network connection. SSL VPNs also let organizations audit IT activity at this level, which HIPAA [Health Insurance Portability and Accountability Act], Sarbanes-Oxley and other regulations now require."

How does IT provide VPNs? "There are two strategies for teleworkers: the hardware approach and the software approach," says Joel Snyder, principal at Opus 1, a Tucson, Ariz., technology consultancy. "Which one is best for a given company and teleworker depends on a number of factors. Is the teleworker doing a single-task job, like tech support, or are they a power user? What's the technical expertise of IT and the teleworkers? Who owns the remote systems, and what is the broadband environment like?"

The hardware-based approach, says Snyder, "involves a VPN box, which the teleworker connects to their broadband modem or home gateway, and then connects to one or more computers and other devices like VoIP [Voice over Internet Protocol] phones." Vendors offering remote VPN hardware clients include Cisco, Juniper Networks and SonicWALL.

With the hardware-based approach, says Snyder, "IT can remotely manage the box and minimize what the teleworker has to manage. It lets IT distinguish between the work and home side of a teleworker's network, and if the box includes Wi-Fi, IT can provide teleworkers with secure wireless." This is important, he stresses, because otherwise teleworkers will set up their own wireless access, "and it won't be reliably secure."

Also, adds Snyder, "The VPN box can support a wider range of multiple devices, like a Windows-based computer, a Mac and a VoIP phone. If a teleworker is using several computers, a hardware VPN is often the only solution that will work. Plus, because VPN hardware tends to not be portable, if the teleworker's notebook is stolen, your network access isn't compromised."

However, remote hardware can be expensive — several hundred dollars per user. By contrast, Snyder notes, "VPN software clients, running directly on teleworkers' computers, are usually provided free."

Both approaches require central VPN capability at the company side, such as a VPN concentrator appliance. The appliance may also support IPsec. Juniper's VPN appliance, for example, "can use IPsec for latency-sensitive applications, VoIP or streaming media where you need the performance, but fall back to SSL seamlessly if a firewall or NAT [Network Address Translation] is in the mix," says Juniper's Ganitsky.

"Products like the SonicWALL SSL-VPN series let you run any application over SSL by tunneling all the traffic over SSL, without needing a pre-loaded client to make it happen," says Doug Brockett, vice president of strategy and general manager, SonicWALL.

Remote hardware can also provide gateway-level security and VPN services. "SonicWALL's TZ series has everything you'd expect to find in a security appliance: firewall, Deep Packet Inspection, antivirus, antispyware, intrusion prevention and content filtering, along with secure wireless and an IPsec VPN option," says Brockett. "The TZ 150 series, for example, allows IT administrators to do remote monitoring and remote threat prevention to these new entry points to the network."

"The VPN to the company network and applications like VoIP, video conferencing and instant messaging have really strong performance issues," advises Opus 1's Snyder. "You can't have any latency or loss, so you need good throughput bidirectionally. This may determine what kind of broadband your users will need to have." DSL broadband, Snyder notes, typically has better-balanced speeds.

For companies who want to provision telecommuters with VPNs, but aren't in a position to administer them, managed-service versions are available, such as Juniper Network's Secure Access SSL VPN product line.

Authentication: Dynamic Passwords

Like any remote user seeking access to your company's network and its resources, teleworkers should be required to authenticate themselves as part of the connection process. A growing number of companies are turning from the traditional "static" password (one that may only be changed every few months, if ever) to "dynamic" passwords, where a new password (an identifying string) is needed each time an employee tries to connect.

A commonly deployed dynamic password generator is RSA Security's SecurID. An RSA SecurID client can be either a hardware "token" like a USB key or a SmartCard, or a software program installed on the user's notebook or handheld computer. Unlike a password, a user can't share the information with a stranger or write it down, since the identifier is only valid for about a minute. Similarly, even if a keylogger script was able to "sniff" the digital string, it would not be useful.

To generate a new identifier, the user first enters a personal identification number (PIN) onto the RSA SecurID pop-up screen, and the SecurID client generates a new authorizing number, which the user then enters into the login box. Inside your company's network, an RSA server, which is compatible with RADIUS (Remote Authentication Dial-In User Service), LDAP (Lightweight Directory Access Protocol) and other leading authentication systems, checks whether the submitted information is correct.

This combination of the PIN and the dynamically changing identifier is called "two-factor authentication," says Karen Devine, director of product marketing, RSA Security. "VPN access is a driving reason for adopting two-factor authentication because of the high perceived risk. For people who work in an office, they've gone through some security simply by coming into the building. Sixty to 80 percent of our customers are using SecurID to secure VPN access."

Most VPN systems support RSA authentication mechanisms, making RSA SecurID easy to add. "With most VPN vendors, when you double-click on the VPN icon, you get prompted for your PIN and token code," says Devine. VPN vendors with RSA SecurID include Check Point, Cisco, F5, Juniper Networks and SonicWALL.

The cost for RSA SecurID typically ranges from $10 to $80 per user, depending on such factors as how many users there are or whether tokens are involved.

Endpoint Security

Because they're outside the company firewall, and often connecting to unsecured networks, remote users' computers are at greater risk than computers inside company offices. Therefore, it is important to implement endpoint security, or checking the security status of "endpoints"— computers, handhelds, smartphones and other devices — when they attempt to connect to the network.

A small degree of endpoint security can be done with any system a teleworker may use — if nothing else, assessing that the endpoint security status cannot be determined, then either refusing access or limiting access to reading and sending e-mail without attachments.

A more comprehensive check would confirm whether the computer is running required security software, whether these programs' signature and rule files are up to date, and also whether the operating system and core applications are properly configured and have all required security patches and other updates.

To make remote systems secure, says Rich Langston, senior product manager, Network Access Control, Symantec Corp., you need to "preinstall an agent program on them, and have central software that ensures it's on and working." To manage all of a company's endpoints, Symantec's Network Access Control (SNAC) offers the central management console, with a single view of policies, says Langston. "When a teleworker connects through the VPN to the company network, using an endpoint running SSEP [Symantec Sygate Enterprise Protection], SNAC will examine the system for compliance with NAC rules. Each time the system attempts to connect through the network, SNAC enforces correct configuration, and can download and install what's needed."

SNAC can be added to your network as a gateway-level appliance. Leading VPN vendors including Cisco, Juniper Networks and Nortel are integrating NAC features into their VPN concentrators, says Langston, so a separate gateway appliance isn't needed. ◊

CDW offers technology service support from top manufacturers
and service providers across all product categories.