Secure Remote Access:
Part 2 — Remote Access Evolves
Global Networking Strategies
David Thompson

Numerous components must be addressed as organizations create and refine security policies for remote access. By 2006, native OS components will replace proprietary software, but those components should be examined now.

Security for remote access currently uses a combination of virtual private network (VPN) client technology and antivirus and personal firewall software. As application access becomes more browser-centric, increasing emphasis should be placed on the end node’s ability to protect itself (see GNS Delta 944, 27 Dec 2001). Organizations must continually re-evaluate the development of this security technology to accurately assess when to deploy new components (e.g., data encryption solutions), as well as to determine when it is possible to discontinue proprietary (and difficult to distribute) software and adopt native OS security capabilities. As native security functions mature and combine with browser-based remote access, it will also be possible to more easily and securely support access from machines not supplied by the company (e.g., employee-owned, public kiosks).

While most corporations are only now examining whether and how to deploy personal firewalls to broadband-connected remote-access workers, during the next two years, personal firewall technology will become the standard antivirus software complement for securing remote broadband-connected user access. By 2003/04, especially as this technology is embedded into operating systems, personal firewalling will become the default minimum (along with antivirus software) for all remote-access users, whether they are dialup- or broadband-based, mobile or fixed telecommuters. Ultimately, the greatest security level can be achieved by applying these same policies and technologies (personal firewall, data encryption) to local users as well as remote users. This requires fully mature technology, or greatly matured OS capabilities, and is not recommended until at least 2004/05 (except in niche high-security areas, or in response to privacy and other regulations).

Current Security Options: Traditional VPN-Based Remote Access

Security options currently include the following:
1. Controlling split tunneling
2. Deploying centrally managed personal firewalls to broadband (DSL, cable modem) users
3. Enabling a personal firewall policy audit

Remote Access Evolves: Next Steps

The next steps in remote access include:

▲ **Firewalling:** Ultimately, firewalls are also required for dialup-based Internet connectivity. Given the relative immaturity of personal firewall products, we recommend that organizations wait 6-12 months before deploying personal firewalls to users to dialup-connected remote workers. Subsequently, it will make sense to address the internal threat by deploying personal firewall technology on the LAN as well. This should not be attempted until management tools are much more advanced (2004+).

▲ **Data encryption:** Encryption at the endpoint is also required to protect sensitive data on remote computers, but due to the almost complete lack of enterprise-friendly solutions — and

**META Trend:** Through 2002/03, investments in perimeter security will focus on implementing intrusion detection systems and improving robustness (high availability, performance, and capacity) of the demilitarized zone. By 2003, as threats proceed up the computing stack and encryption increasingly blinds network-based components, attention will shift to special-purpose firewalls/proxies and multifunction, node-centric solutions. Maturing by 2005/06, such solutions will lead to the dissolution of traditional perimeters.
as other required infrastructure components (universal OS support of encryption, PKI to manage keys) are still developing — organizations are advised to wait 12-18 months, at minimum, before making encryption a standard practice. Limited deployments of encryption technology to protect critical data are still advisable, but operational costs will be high. Organizations should examine extending these controls into the enterprise (to desktop computers on the LAN) during 2005/06, and earlier if they face regulatory privacy requirements (e.g., HIPAA, GLBA, EU regulations; see GNS Delta 878, 19 Jun 2001).

Remote Access Evolves: Native OS Support

Windows XP includes not only the IPSec VPN client of Windows 2000, but it contains a basic personal firewall as well. Since Win2000, there has also been capability for data encryption using Encrypted File System (EFS). Organizations should continually examine the native OS support for requisite security functions (VPN, personal firewall, data encryption), but must keep in mind the relative immaturity of the offerings from Microsoft. While the VPN and personal firewall components provide basic functionality of establishing VPN tunnels and blocking (some) ports, absolutely no central control exists in the current environment. Microsoft lacks even the basic ability to centrally define and enforce a split tunneling policy, let alone do more complex management of VPN and firewall policy. On the encryption front, EFS supports a basic and manual data recovery process, but no key archive or recovery tool — again highlighting its immaturity. Thus, although upfront costs will be low (no software to purchase or distribute), support costs will be very high, and there will be no way to confirm policy compliance. As such, organizations should not base large-scale security services (for more than a few hundred users) on native Microsoft functionality until at least 2004.

Remote Access Evolves: Flexibility of Home Use

As companies refine their remote-access policies, the dilemma of whether to support the use of home-owned computers is being re-examined. With current fat-client deployment scenarios (e.g., based on third-party VPN clients, personal firewall code), the problems of support are quite significant. Because the IT organization has no real control over the OS or image of the computers in question, we have long recommended against this practice because the cost of support for such users quickly overwhelms the relatively low cost of a Wintel box (see WCS Delta 641, 1 Jul 1997). However, many organizations wish to support occasional home workers (often due to executive mandate), and if there is no other alternative, the security manager must at least ensure that the basic security policy (antivirus, personal firewall, authentication, encryption) is being met in all environments. At the very least, steps taken must include the following:

▲ The distribution of a separate, employee-signed policy document that acknowledges the employee’s awareness of the specific remote-access security requirements
▲ The documentation of what specific tools will be used to meet policy requirements, whether owned by the employee or provided by corporate (e.g., antivirus packages, firewalls)
▲ The definition by the IT organization (and approved by management) of the level of support that employees can expect on non-corporate resources

Longer term, the advances in native OS support and browser-based remote-access functionality will enable flexible and secure access from various machines (kiosk, home owned, etc.), but this should not be expected until 2005/06.

Bottom Line

The security technology required to support broad-based remote access will be principally provided outside the operating system. Native operating system remote-access security will not mature until 2005/06.

Business Impact: Efficiency and productivity is served by enabling more flexible access to corporate resources. However, organizations must realistically assess the management weaknesses and resulting high support costs when deciding on remote-access models.