Secure Remote Access: Part 1 — Best Practices. Given changing threats, remote-access mechanisms, and technology solutions, organizations are struggling with how to secure the numerous computers used by employees for remote access. Companies must develop a multifaceted remote-access strategy to encompass all permutations.

META Trend: Strengthening and centralizing authentication/authorization services are becoming top security concerns as organizations bolster e-business (external) security architectures and rationalize with internal solutions (2001-03). Traditional boundaries will melt as security functions (e.g., intrusion detection, firewall, PKI) are increasingly embedded in infrastructure components during 2002-04.

Organizations are attempting to control the security exposure introduced by remote-access mechanisms, but they face a rapidly changing environment that complicates solutions. The various computing devices, access facilities, connectivity interfaces, and associated security threats make the simple decision of whether to deploy technology, such as a personal firewall, incredibly complex. Organizations must rationalize their remote-access security policies to provide safe and increasingly flexible remote access to corporate resources via multiple channels (e.g., virtual private network [VPN], Web, wireless).

Although most corporations are only now examining whether and how to deploy personal firewalls to broadband-connected remote-access workers, during the next one to two years, personal firewall technology will become the standard complement to antivirus software for securing remote access. As this technology is embedded into operating systems, there will also be significant deployment of Web applications to support browser-only remote access. By 2004, 50% of remote access will be via Web browsers and increasingly accessible by wireless mechanisms, as well as wired. This will place incredible stress on current authentication practices, because user name/password is not sufficient — in terms of security or manageability — in this environment, and will necessitate sophisticated mechanisms to manage user identity (e.g., PKI, Kerberos, Passport). However, not until 2006 will it become common for employee portals to be fully externalized.

Users must examine the security options available for traditional VPN remote access, as well as for Web-based access. Organizations should focus on protecting the core enterprise network, remote computers, and any data that resides on them; it is assumed that antivirus software is already deployed (see GNS Delta 771, 23 May 2000).

Security Options: Traditional VPN-Based Remote Access

- Controlling split tunneling: The most basic level of security that can be provided is to control split tunneling within the VPN client. With split tunneling disabled, a VPN user cannot simultaneously connect through the VPN to the enterprise network while browsing the public Internet. This basic level of security is often sufficient for modem-based Internet connectivity and, if combined with strong two-factor authentication, can go a long way toward locking down the core network if not the remote computing device and data. As Windows 2000/XP becomes more pervasive, organizations will actually

Business Impact

Increased efficiency requires flexible access by employees to corporate resources, but the risks associated with such access must be weighed along with the costs of mitigation.
lose this control when native Windows functionality acts as the VPN client (during 2002/03).

- **Deploying centrally managed personal firewalls**: To increase the protection of the remote computer (as well as the core network), especially when users are connected via broadband or always-on mechanisms (e.g., DSL, cable modem), organizations should evaluate personal firewall technology (see GNS Delta 832, 16 Jan 2001). In a corporate context, organizations should focus only on solutions that enable central policy control and definition. With the presence of a centrally configured firewall, it is also possible to reassert split tunneling controls. Split tunneling requires that all Internet traffic be backhauled through the VPN and out the corporate firewall (if browsing simultaneous to VPN connectivity). This has significant bandwidth implications, but the presence of a personal firewall can mitigate the risk of direct Internet access. However, the most security-conscious organizations are still advised to keep split tunneling off. The execution of security policy on the client (the firewall, AV, etc.) will also be embedded in operating systems during the next few years. It will become fully subsumed by 2004, but will still require separate and central management (the next step).

- **Enabling personal firewall policy audit**: Beyond deploying a centrally managed firewall, organizations need some mechanism to ensure that the code (running on common Windows operating systems) is actually functioning in accordance with policy. Numerous mechanisms exist to do this, including integration of an audit-checking tool with the VPN gateway (e.g., Checkpoint), a standalone network device (e.g., InfoExpress), or direct integration between the firewall and VPN code or even OS — so that if the firewall is changed or disabled, either the VPN (e.g., Cisco with ZoneAlarm or BlackICE) or Internet (e.g., BlackICE) connectivity is disabled. Ultimately, by 2004/05, this functionality for policy definition and enforcement will become a portion of a security management console dedicated to the configuration of control points on the network (e.g., firewalls, personal firewalls, VPNs).

**Remote Access Evolves**

The frequent requirement to support home-owned equipment, combined with the overarching desire to provide more convenient and flexible access to corporate application resources (especially e-mail), has led to the recent development of Web-based remote services. E-mail and collaborative applications have been the first to be “opened” to the Web, but many portal applications currently on intranets will be externalized during the next two years (see GNS Delta 874, 5 Jun 2001). Ultimately, wireless remote access will follow this same pattern. From a security perspective, the primary consideration is the fact that it is not possible to deploy client security software (e.g., antivirus, personal firewall), nor is it possible to trust the integrity of the client computing platform in any way. This necessitates locking down the session as tightly as possible, which means SSL for encryption combined with the strongest authentication possible. Two-factor authentication tokens are the best candidates (e.g., RSA SecurID, Vasco Digipass, Secure Computing SafeWord), and an absolute requirement for any application with sensitive corporate data (including e-mail access). It is also advisable to deploy intrusion-detection technology at the head end to provide a “backstop” at the central site. This helps ensure that if a session is compromised or the Web-accessible server is hacked, such an intrusion can be detected and a penetration of the network prevented.

Organizations should select from among the available options based on business (and thus application-specific) requirements. An analysis of the trust of the users, network, and applications versus the security risks can highlight the strength of the solution required (see GNS Delta 789, 1 Aug 2000).

**Bottom Line**

A series of different security steps should be taken immediately to protect remote access, but organizations must also consider the future and evaluate security strategies, given Web and wireless access mechanisms.