Global Networking Strategies
David Thompson

Organizations must develop a repeatable process for matching technological solutions and user requirements to establish set usage of remote access mechanisms. As technologies mature and new options emerge, this process of user analysis should be repeated periodically to ensure the best combination of security, flexibility, and cost for the numerous employees requiring remote access.

We have examined numerous technical solutions to the remote access (RA) conundrum and introduced the concept of providing different types of access to different user groups (see GNS Deltas 944, 952, and 1008). Organizations must evaluate user RA requirements to select the best possible solution for different users. This process consists of two steps:

1) Segmenting the user population into different groups, organized by similar requirements and based on analysis of who the users are, what applications they need access to, where they need access from, how they gain access (from what devices), and the security requirements associated with that access
2) Matching user groups to different technology options by determining the best combination of security, flexibility, application support, and cost

By 2004, best-practice organizations will perform a comprehensive analysis of RA requirements by categorizing users and selecting appropriate solutions. But this will not become common practice until 2005/06, and alternative access mechanisms initially will be deployed in an ad hoc fashion (e.g., Web-based e-mail). By 2006, remote access will be much more pervasive, driven by the efficiency gained in migrating to Web-enabled corporate applications. By 2007, multiple device types and 3G wireless networks will further emphasize the need for a comprehensive RA strategy by providing new, more flexible network and device alternatives. This trend is beginning now with 2.5G wireless, RIM (Research In Motion), and other dedicated networks.

User Profiling

Users will be categorized based on specific criteria, including:

▲ **Usage model (“who”):** First, organizations must examine who requires RA as well as the usage model associated with the access. For example, the usage models for dedicated RA workers and those for occasional weekend users differ substantially. The casual user does most of his or her work in the office, and the expense of dedicated RA computing hardware (a laptop or second PC) is not justified. Similarly, the significant expense of supporting RA tools such as virtual private network (VPN) clients, personal firewalls, antivirus software, and security policy managers is also not justified. A casual user is an excellent candidate for Web-based RA, whereas a dedicated remote worker justifies the full investment of PC hardware and security software (VPN, personal firewall, etc.). By 2004, 33% of Global 2000 organizations will support Web-based remote access for some segment of their users (60% will do so by 2007).

▲ **Application support (“what”):** Next, the IT group must examine the applications to which users require access. Some users require only basic e-mail or intranet/Web access, while others require more sophisticated access (e.g., ERP systems, even direct access for network management). Web-based solutions, however, inherently limit (even further than the VPN model) the types of applications that users can access to those applications that have a Web interface or...
can be connected to an HTTP proxy. Planners must therefore keep in mind the constraints of the various access mechanisms.

▲ **Flexibility (“where”):** Planners should also examine the location from which users connect. Organizations must evaluate whether the users are highly mobile, operate from a fixed location, or represent a combination of fixed and mobile user. Client software inherently limits the flexibility of the RA solution, preventing connection from any computer that lacks the security software, and often preventing connection from behind firewalls. Highly mobile workers, even if they carry corporate laptops, may require connections from behind firewalls (e.g., on a foreign network). This RA requirement is more easily met with SSL connections (because firewalls almost never block outgoing SSL) than with VPN technology (which is frequently blocked, and which has difficulty with NAT traversal). Because there is still locally resident data that must be protected, the use of SSL does not mean that personal firewalls and other client software can be neglected.

▲ **Platform (“how”):** Although initial plans may support only PCs (laptops and desktops), organizations must keep in mind the emerging demand for PDAs and other devices (RIM, pagers, etc.). While the same security issues and requirements exist (as for personal firewalls, antivirus software, etc.), the solutions for constrained devices are much less mature. Organizations must continually re-assess security requirements in this area, as well as the status of technical solutions (see GNS Delta 771).

▲ **Security/sensitivity requirements:** Client software such as VPN clients, personal firewalls, and antivirus is required to achieve the highest levels of security. Native operating system support for VPN clients will mature and become widely deployed by 2004/05. Yet security policy management tools are also required to ensure these services are functioning, and encryption tools may be required to fully protect stored data. Client-less models currently cannot protect the end device or the integrity of a session — and likely never will, at least not in a fashion that corporate IT groups can control or monitor. For some applications, client software will be essential, regardless of flexibility and other requirements. In some cases (when there is absolutely no locally resident sensitive data), personal firewalls and antivirus software can be left out of the solution, as long as authentication methods are adequate to protect the network itself (e.g., use of strong token- or smart card-based systems). In these cases, however, it is entirely possible that the contents of any individual session could be compromised.

This usage analysis must then be applied to different user groups and populations, allowing remote access solutions and user requirements to be efficiently mapped. Figure 1 following provides an example of analysis that is applicable to most users. This is not intended to be a comprehensive example, but instead demonstrates the typical categories that can be used as a starting point for an in-depth analysis.

**Bottom Line**

To perform a comprehensive analysis of user remote access requirements and appropriately match the questions of who, what, where, and how regarding the various remote access technical solutions, organizations must use a process-based approach.

**Business Impact:** Categorization of remote access users and solutions will enable the most efficient resource allocation for remote access support, and will also prevent organizations from forcing improper solutions on an increasingly diverse and mobile user community (including business partners). Without a formalized process, remote access will result in high support costs and security breaches.
The user profiles noted below and in the table following represent typical cases. This list is not intended to be exhaustive, but serves as a starting point for more detailed analysis of user types specific to an organization:

1) **Dedicated Home Worker:** Includes workers whose primary work location is a fixed location such as a home office. These users should certainly be provided with a corporate computer. Given that standard hardware and corporate desktop software images exist, supporting security software is not nearly as difficult to provide as for home-owned PCs. Furthermore, because users will most likely store applications and data locally, we absolutely recommend the use of VPN clients, personal firewalls, antivirus software, and security management tools. File encryption requirements vary according to the sensitivity of the data. Eventually all remote workers should use personal firewalls, with broadband-connected users receiving priority. Part-time fixed remote users are a special case of dedicated home workers; these users will need multiple profiles depending on whether they are working from the office or home.

2) **Casual Remote Worker (e-mail access):** For these users, specialized hardware will rarely be deployed, because most of the time, this user is using a desktop on the corporate LAN. Organizations are just now encountering the difficulty of supporting security software on home-owned equipment. We recommend evaluation of Web-based RA, in conjunction with Web enabled e-mail, but ONLY if strong authentication mechanisms are used.

3) **Casual Remote Worker (IT administration):** These users require functionality from their access that Web interfaces cannot support. Although IT support staff usually work from an office, administrators frequently need remote access to quickly address a problem. Because administrative access to systems is highly sensitive, strong authentication is a must. Due to the nature of the access needed (to SSH or Telnet, or similar remotely managed resources), Web access will not be sufficient. We recommend VPN-based mechanisms and the use of either a laptop as the primary corporate machine, or alternatively a dedicated "on call" laptop shared among IT staff. Personal firewall and antivirus software should certainly be evaluated, but the disabling of split tunneling (see GNS Delta 944) will likely be adequate as it is unlikely that there is sensitive data resident stored locally.

4) **Mobile Worker:** A mobile worker (or "road warrior") will most likely be issued a corporate laptop, and just as for fixed remote workers, we recommend that VPN, personal firewall, and antivirus software be used. Traveling workers may also require Web-based mechanisms to enable access when sitting behind a firewall on a foreign network not under their control (e.g., a salesperson or technician connecting from a customer LAN). Because such firewalls are often configured to block IPSec traffic, VPNs alone may not be sufficient. This does not negate the requirement for personal firewalls, antivirus software, etc., because the data resident on the machine must still be protected.

(cont.)
<table>
<thead>
<tr>
<th>Usage Model (Who)</th>
<th>Application (What)</th>
<th>Flexibility (Where)</th>
<th>Security (How)</th>
<th>RA Model</th>
<th>File Encryption</th>
<th>Connectivity Model</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fixed Remote</strong></td>
<td>Dedicated remote employees (e.g., remote call center)</td>
<td>All or many applications (CIC, CRM, e-mail, etc.)</td>
<td>One location, corporate-provided PC</td>
<td>Must be Secure</td>
<td>VPN, personal firewall, antivirus policy enforcer</td>
<td>Recommended for sensitive data</td>
</tr>
<tr>
<td><strong>Casual Remote, General</strong></td>
<td>General user; internal employee desiring e-mail access</td>
<td>E-mail, Web HR applications</td>
<td>Primarily home access, but flexible access as indicated by mgmt.</td>
<td>Medium security; e-mail is sensitive, but no locally resident data</td>
<td>Web/SSL, client-less</td>
<td>No (nothing to encrypt)</td>
</tr>
<tr>
<td><strong>Casual Remote, IT Staff</strong></td>
<td>IT users requiring access for on-call trouble shooting</td>
<td>Diverse, trouble-ticketing application, network monitoring application, SSH, etc.; connection to network devices</td>
<td>Primarily home access; on-call access required anywhere</td>
<td>High security; user has access to change network settings</td>
<td>VPN, personal firewall, antivirus policy enforcer</td>
<td>No (no resident data to encrypt)</td>
</tr>
<tr>
<td><strong>Mobile Remote</strong></td>
<td>Mobile sales workers</td>
<td>Highly mobile; home access and access from the road (hotel, client site, etc.)</td>
<td>High security; user has access to customer data, price lists, etc.</td>
<td>Personal firewall, antivirus policy enforcer, and VPN or SSL as required</td>
<td>Yes, recommended for locally stored data (price lists, customer lists, etc.)</td>
<td>Yes, recommended for locally stored data (price lists, customer lists, etc.)</td>
</tr>
</tbody>
</table>

Source: META Group