Global Information Assurance Certification Paper

Implementing Remote Access; Security, Usability and Management
John Torello
6/11/01

In case you haven't noticed, the days of working 9:00 to 5:00 at the office have been coming to an end. These days, most of us are actually working more than the traditional forty hours per week. This certainly isn't a new trend. What *is* changing is the amount of time the average person spends *at the office*. Technology has enabled us to connect to our corporate LANs from our homes, from hotels while on business trips and even from the pool or beach while on vacation. Telecommuting, the term often used to describe remote access to the corporate LAN, has enabled many workers the ability to have much more flexible work schedules. Telecommuting especially makes sense for the "remote work force". These are the folks, like salespeople, who are on the road for a majority of the time and don't have regular access to a traditional desktop PC. In addition, many companies now have employees working on flextime schedules, where they work part-time from home.

Employees aren't the only ones benefiting from this arrangement. With VPN technologies in place, companies can save significant amounts of money in leased line and other infrastructure costs. Some companies are even spending less for expensive office space by having employees work from home. "According to Infonetics, a networking management consulting firm, LAN-to-LAN connectivity costs are typically reduced by 20 to 40 percent over domestic leased-line networks; cost reduction for remote access is in the 60- to 80-percent range."[1]

So, telecommuting and flexible work arrangements seem to be a great solution in an age where we are all trying to get more and more accomplished in less and less time. The challenge is to implement a solution that is secure, has acceptable performance and is reasonably simple to use and manage.

The Problem

As with most technology solutions, one size doesn't fit all. Companies have disparate workforces, applications, and security and network architectures. All of these factors can make it difficult for companies to easily implement end to end solutions when it comes to remote access. Let's face it, maintaining a secure LAN already takes a tremendous amount of time and effort. With the implementation of remote access to employees and corporate partners, we have additional considerations.

Firstly, we don't have direct control, at least in the traditional sense, of employees working from the road or at home. Nor do we have control over business partners working from their own offices. To make matters worse, more remote users are taking advantage of high speed Internet connections as availability and affordability of these services continues to increase. "Market Research Company International Data Corp. predicted that there will be more than 20 million broadband users in the United States by 2003. Sixty-four percent of those users plan to use broadband for remote access to corporate networks, IDC reported."[2] The problem with broadband from a security perspective is that these "always on" connections put users' PC's, and therefore the corporate LAN, at risk twenty-four hours a day. "Remote PC's connected to the Internet via DSL and cable modem services can be linked to the network all

the time, yet they lack the protection and policy enforcement of a corporate firewall, according to security experts. Without adequate protection, these PC's are exposed to hacker attacks through their virtual private connections."[3]
Security is not the only issue. I.T. managers must consider network and application performance, usability, connectivity flexibility, and ongoing management and support when considering a remote access solution.
As with any I.T. projects, doing your homework and planning carefully will ultimately reap rewards. Don't rush a solution into place. There are five key elements to consider when planning a secure remote access solution.

1. Initial Assessment; Understanding the Business Need

   This is an area that tends to get overlooked when planning a remote access solution. It is critical for I.T. staff to have a solid understanding of the "who, what, where and why" of the end user community when it comes to remote access. All too often we focus all of our energies on the "how". It is important to understand that the technology is only one part of the overall remote access solution. Also, knowing what your end users REALLY need to have access to may affect your security architecture and configuration.
   A good place to start is to review all current connections into (and out of) the corporate LAN. For the sake of this discussion we will use a single location with multiple remote connections as an example. You want to identify all of your remote users and determine how they are getting to your network. This assessment should include:
   - Direct dial-in to a modem pool/RAS server
   - Direct dial-in to the desktop PC
   - Dial-out from the PC
   - FTP or HTTP Electronic Data Interchange (EDI) with trusted partners
   - Existing leased-line connections
   - Existing Virtual Private Network connections

   This may be a fairly simple and straightforward task in a small organization. In larger organizations though, there may a number of "exceptions" to the general rule.
   Next, you need to get an understanding of what systems and applications your end users are connecting to. Whatever technology solution you decide to implement, you will need to test and benchmark your company's critical applications. Keep in mind that different applications will perform differently under various circumstances. Encryption will impact the performance of your applications.
   Finally, you will need to understand the number of users that will be accessing your network remotely. You need to consider both total numbers of users as well as numbers of concurrent users. It is a good idea to poll internal departments and assess external partners to get a reasonable estimate of both current and future needs. Scalability of the remote access solution should be a factor in the decision making process.

2. Planning a Technology Solution; Considerations

   Hopefully, if you've done your homework during the initial assessment phase, you should have a good understanding of who needs to access your network and how they will access it.

Consider the following points with the technology solution.

- The solution needs to be flexible enough to support different connection types. Remote users and business partners may be connecting to your network via a variety of methods including, dial-up, DSL, cable modem, point to point data connection (T1) or wireless connection. The remote access solution needs to be able to accommodate different methods of connectivity without making it difficult to manage and support all users. However, regardless of what combination of hardware and software utilized, the most important point is to maintain a centralized access point into the network. If the plan is to have remote users go connect via VPN through the firewall to get to the LAN, then avoid setting up any direct dial-in lines to desktop machines. Every exception to the general rule is a potential back door into the network. These exceptions make it significantly harder to maintain and monitor the remote access environment.

- Configuring the central point of access (the remote access server/device) is key to the overall security of a remote access solution. Only services that are absolutely needed for end users to conduct business should be enabled. In the case of a Remote Access Server (RAS), any software that is not needed should be uninstalled. In addition, end users should not have access to any locations on the RAS server, and should only access and save data to and from appropriate locations on the network. It will be necessary to lock down the file system on the server so only administrators have access.

- Ideally, remote users should be authenticated and authorized with the existing means of network authentication and authorization. It is preferable to find a solution that doesn't require an additional layer of authentication. Users that have to remember multiple passwords tend to use simple (easily guessed) passwords, or they will write them down and leave them on their PC. This type of activity creates an internal security threat.

- Securing the data that is passed from the remote user to the corporate LAN server is another critical component of a remote access solution. There are three key considerations here.

1. Session Security; A VPN "tunnel" should be established from the client (remote) device to remote server. This session will allow for a level of end to end security between the remote client and the server. The IPSec standard is an example. Packet authentication is also a consideration to ensure the integrity of data passing to and from the remote client and server.

2. Data Encryption; The packets being sent over the VPN tunnel should be encrypted. In this way, if packets were to be intercepted, they would have to be de-crypted to be of use to an unauthorized user. 3DES is one example. In order to have the highest level of data integrity completely from end to end, also consider encrypting the data on the local drives of both the remote device and the server (if data is stored there). Data left "unprotected" on the local drives of these devices is vulnerable to hacker exploits, so encrypted tunnels are only part of the solution for companies looking for the highest level of security.

3. Security of Remote Devices; The physical security of remote computers and devices is as important as protecting the data that passes between them. Laptops and PDAs can be easily lost or stolen. Company policy should dictate that confidential information NOT be stored on local drives of remote devices. If it is absolutely necessary to store data locally, then the data should be encrypted. The security of portable devices can also be enhanced through the use of smart cards and biometrics devices. Remote devices also need to be protected from viruses and other hacker exploits.

- Protecting the network from viruses and other malicious code is a critical component in ensuring a secure remote access solution. The remote access server, as well as the remote devices, should have anti-virus software installed and kept up to date with the newest anti-virus definitions. Symantec, the company that makes Norton AntiVirus, has reported over 49,000 viruses and over 20 new viruses in May 2001 alone.[4] Viruses, Trojan horses and malicious executables are becoming more dangerous and prevalent. These days, there is a lot more to worry about than just Microsoft Word macro viruses. Programs such as Back Orifice allow the hacker to access and control the victim's machine. These types of programs have dangerous implications to unprotected machines connected to corporate LANs. Since new viruses and malicious tools are being created almost daily, I.T. managers must ensure that remote users are maintaining the latest virus definitions on their remote devices. The remote access solution should have a component that allows for centralized management and configuration of remote devices, so that software updates such as anti-virus definitions can be rolled out without end user intervention. Unfortunately, you cannot rely on your remote users to keep their security configurations up to date. "Technologies such as anti-virus software tend to be less rigorously updated, and others, such as encryption, are hardly used at all, even if they're used at work, experts said."[5]

- Remote users connected to the Internet must also protect their machines from hacker exploits. Personal or "distributed" firewalls help protect remote devices that are connected to the Internet. A distributed firewall that can be centrally configured and managed is the best way to ensure protection for devices outside of the corporate firewall. Without this level of protection, an attacker could conceivably take control of a remote device and ultimately get to the corporate LAN.

- Performance and usability are always issues when addressing secure remote access solutions. Today's applications are more robust, requiring more resources to run them efficiently. Some of these applications are already too slow for end users on the LAN, without adding layers of encryption to slow things down further. Users working remotely expect that they will be able to get to what they need quickly. Usability is a big concern for end users. One of the biggest issues facing end users when VPN technologies were first implemented was ease of use. Many end users had difficulties installing, configuring and updating VPN client side software. Security solutions like smart cards, certificate installs, VPN client installs and biometrics can all be frustrating experiences for both the remote user and I.T. manager if not properly implemented. This poses the common problem to I.T. managers in finding a solution that is both efficient and secure.

Certainly, cost is a consideration when planning a secure remote access solution. Distributed firewalls, anti-virus software for remote devices (that may not be company owned), VPN client software and monitoring tools such as Intrusion Detection Systems (IDSs) are all additional costs that are sometimes not considered in the initial planning. Depending on the size of the organization, these items can add up to a substantial sum.

3. Policy and Procedure

Creating and enforcing the appropriate policy and procedure around remote access can be a difficult task. Ideally, technology will dictate and enforce the policy. For example, if your policy dictates that end users may not access the network remotely after 11:00 PM, you can enforce that policy simply by restricting log-ins after 11:00 PM. However, not all policy is enforceable through technology. There will always be a human factor involved. Therefore, it is important to have policies and procedures that meet the following criteria:

- The policy and procedures are documented, and in a concise and easily understood manner
- The policies are enforceable, and hold end users accountable where appropriate
- The policies should be in-line with corporate standards and should be supported by the Human Resources department or other appropriate business area

Specifically, the remote access policy and procedure document should address the following areas:

- How one initiates a request for remote access
- How one gets approval for remote access
- Which devices are acceptable for use, and what methods of connection are acceptable
- What specific tasks or items are end users responsible for
- Where is data stored, and what restrictions are there regarding storage of confidential data
- What levels of encryption are being used
- When can individuals access the network, and what is accessible
- How do end users report technical problems and what level of support can be expected
- Applicability to the company's Corporate Confidentiality Policy
- How do end users report security issues (theft of equipment, security breaches, etc.)
- How departing employees remote access accounts removed
- What level of financial support (if any) is the company willing to provide for set up and ongoing communications charges

All of these items must be clearly defined before a remote access solution should be rolled out to the end user community. The remote access policy and procedure document should be carefully reviewed in user training sessions to ensure the best chance for ongoing compliance.

4. Training and Support

As with the assessment phase, training and ongoing support is an area that can make or break

the overall success of the implementation. Training end users and business partners can be a difficult and frustrating process. The problem lies in the fact that most remote access solutions require some setup and configuration from the end user. Life becomes somewhat easier if the remote devices are all portable, but many may be using equipment that is always offsite. Even the largest help desk operations cannot visit employee's homes to set up the corporate VPN client software! This especially poses a problem to companies whose employee population is not very savvy with technology. There are a few things to keep in mind in order to maximize chances for success in this area. Firstly, make end-user training mandatory before access will be granted and be certain that the end user community has the appropriate expectations in terms of setup and training time. Be sure that the policy and procedure document states this. The "Friday at 5:00 PM" remote access requests are going to occur – know how to deal with them.

If setup and configuration is required by the end-user, make sure to have step by step instructions that are very clear and concise. Instructions with screen captures tend to work best. During end user training sessions it helps to walk through the setup step by step with the instructions. Remember that many end-users may have never seen dial-up or other configuration settings before, and they may have never installed software on their PC before. Don't take anything for granted.

Finally, make sure internal support staff are appropriately trained. As with any other new implementation, they will receive calls that have never been addressed before. New issues need to be logged, escalated and resolved. End users should be updated of potential issues that may affect them. It is also good practice to send regular security reminders and "best practices" to remote users so that network and remote security is a topic that is always fresh in their minds.

5. Monitoring and Auditing

Business solutions like telecommuting for employees and Electronic Data Interchange between partners create circumstances where inbound access to the internal network from the Internet is an acceptable action. Obviously, this makes monitoring activity on the LAN trickier, and ongoing management of the solution requires resources. Monitoring, reporting and auditing can be a daunting task for smaller organizations with limited I.T. resources. There are many tools to choose from. Consider these points to keep the monitoring and auditing process as simple as possible.

- Maintain a homogeneous remote access environment. Avoid "exceptions" in terms of access points. Manage remotes access from a single device.
- Leverage the Remote Access Policy. The Remote Access Policy will define what is acceptable and expected behavior in terms of remote activity.
- Understand your entire network. A successful monitoring and auditing program depends on a "known state". It is critical for I.T. to have a solid understanding of the edge of the network.
- Implement a solution that gives you the ability to monitor and report on the system in a reasonably simple and efficient manner. Be sure the management and monitoring tools used will work for your organization.

If outsourcing the monitoring and reporting of remote access is a consideration, make sure your partner understands your environment, and can provide you with the data and support that is expected. Support and maintenance are the areas where outsource partners will differ the most.

Finally, organizations need to define how incidents will be handled. It is prudent to create an Incident Response Team as well as specific Incident Handling Procedures. It is important to hold internal employees accountable for policy violations. All incidents should be documented and brought to an acceptable level of resolution, as defined by the Incident Handling Procedures.

Issues and Challenges for the Future

Technology is a wonderful thing. It has enabled us to be much more flexible in the way we work. Our computing devices are continually becoming smaller and smaller as microchip technology continues to evolve. However, these innovations come at a price. "According to Psion, around 75,000 people received handhelds for Christmas, and the company has warned businesses to put policies in place to prevent security and management nightmares as users attempt to connect to their corporate networks. Psion said that risks to businesses include the loss of sensitive company information as users download data from their PCs, and network crashes as the extra data traffic generated by the devices causes bandwidth overload."[6] Data integrity issues have dollar values associated with them. "As more professionals, managers and executives have taken their PCs and other mobile devices on the road to keep up with competitive e-business pressures and as telecommuters working from home have proliferated, security breaches traceable to mobile workers have begun to cost enterprises real money. In fact, security problems related to telecommuting contributed to the $66.7 million in losses due to theft of proprietary information identified in a 1999 survey of 273 companies conducted by the Computer Security Institute and the FBI."[7]
We continue to become more of a mobile workforce, and the devices we utilize to connect become smaller and more capable. This poses a continuing challenge to I.T managers to ensure that our private data remains private. I.T. managers and administrators will need to have a solid understanding of Internet security technologies as our corporate networks continue to extend to our employee's homes and our partner's offices.

---

[1] "Reference Guide-A Primer for Implementing a Cisco Virtual Private Network." 28 Aug 2000. URL: http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm (1 Jun. 2001).

[2] Yasin, Rutrell. "Telecommuters On Security Alert." InternetWeek. 3 May 2000. URL: http://www.internetweek.com/story/INW20000503S001 (20 Apr. 2001).

[3] Yasin, Rutrell. "Telecommuters On Security Alert." InternetWeek. 3 May 2000. URL: http://www.internetweek.com/story/INW20000503S001 (20 Apr. 2001).

[4] URL: http://www.symantec.com/avcenter (1 Jun. 2001).

[5] Berinato, Scott. "Do Telecommuters Invite Intrusions?" eWEEK. 17 Nov. 2000.
URL: http://www.zdnet.com/intweek/stories/news/0,4164,2655595,00.html (5 Jun. 2001).

[6] Ticehurst, Jo. " Security warning over PDAs at work." 15 Jan. 2001.
URL: http://www.vnunet.com/News/1116334 (5 Jun. 2001).

[7] Chen, Anne. "Wolves at the door. Stopping big, bad hackers from targeting mobile workers." eWEEK.
4 Dec. 2000. URL: http://www.zdnet.com/eweek/stories/general/0,11011,2658180,00.html (8 Jun. 2001).

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS