GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Remote Access: Opportunities and Considerations

Submitted by: Jennifer Greeley
Assignment: Version 1.3

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Employers of today are drastically different from the employers of yesterday. They understand the responsibilities that come with families and the efficiency and cost savings that working from home can bring. It has also been suggested in the press, that since the attacks of September 11th, greater importance will be placed on remote access,[1] since the possibility exists that whole offices could be wiped out in a matter of minutes, not only from terrorist attacks, but also from natural disasters. To provide the capability of accessing crucial network resources from the confines of one's home, the IT manager has several options which depend on many variables. It can be a large endeavor. This paper will explore the development of a business case for providing remote access (specifically via a VPN), security features provided by the VPN mechanism, monitoring remote access once it is installed, and finally the remote access policies that should be implemented.

Developing business cases is a crucial part of any IT manager's job description. Business executives require clear business reasons for acquiring new technologies. In the case of remote access, there will almost always be clear benefits to providing this service to employees. However, implementing remote access can be confusing and time consuming. The IT manager must decide the mechanism for delivering this service and, assuming it is a VPN, how the VPN will establish connections with remote users. Two alternatives include client-initiated tunnels and Network Access Server-initiated tunnels (via the user's ISP). The IT manager must decide which method is right for their organization based on several variables, including cost, as well as the politics of the organization. Of course, once remote access is implemented, maintenance will be necessary, including the setting of policies and policing of activities.

Developing a Business Case for Remote Access

Many IT departments are faced with employees begging for access to network resources from home. However, is it worthwhile for your organization? Sometimes it can be especially difficult to justify technology expenditures to upper level management when it appears that technology is constantly changing and in need of replacement. Therefore, in developing a business case for new technology, a strong argument is essential. Companies should consider the following when deciding if Remote Access is necessary for the efficiency of their business and the retention of their employees:

- **Consider the nature of the company:** Do most employees' job functions require them to have access to network resources? Is it feasible, based on the nature of the business, that employees will be able to work efficiently from home? What kind of files will the user be accessing? Will they require access to large files, which if they are using a dial-up Internet connection, will ultimately result in failed downloads or extremely long download times?

[1] Brewin, 1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- **Consider the nature of the employees:** Do most employees leave their work at the office? In other words, given the opportunity, would employees choose to login from home to do additional work? Are employees staying late as it is to get work accomplished that can only be done on the network?
- **Competition for employees:** As companies become more competitive for talented people; as they strive to become number one on the Fortune list of best companies to work for, they will look for ways to entice those talented people to work for them. One way is to ensure that family oriented employees can work from home when necessary. Is the company attempting to lure intelligent people away from other companies?
- **Travel:** Do employees travel for extended periods of time? Do they often need access to the network when out of town on business?
- **Customer focus:** For some companies, the bottom-line is the customer. Will providing remote access somehow enhance customer satisfaction? For instance, in the sales industry, the use of remote access would allow a salesperson who has been traveling all day to login at night and use network resources to create sales quotes for potential customers or login to a research database to identify new markets. Increased customer response time will also result. For consultants out in the field, accessing corporate information or other technical data, not only improves efficiency, but increases the consultant's value in the eyes of the client.
- **Cost:** Will the benefits outweigh the costs of the access? Just how much will it cost? What hardware will need to be acquired? What software?

The decision to implement remote access should consider all of these points, since managers will want to know the answers to all of these questions. Providing clear and concise information will make the decision, as well as implementation, an easier task. Once the decision has been made, in depth implementation and configuration plans should be explored.

When deciding to implement remote access, most companies at least investigate the option of VPNs. In contemplating whether a VPN is right for your organization, consider the crucial factors that impact the success of a VPN implementation. These include:

Crucial Factors		
Current IT Staff	***Network Capacity& Infrastructure***	***Costs***
Is there enough staff to maintain the VPN?	How many employees will need remote access?	Will additional staff need to be hired? If so, at what cost?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Crucial Factors		
Does the current staff have the knowledge to implement the VPN and then maintain it, i.e manage the encryption and maintain tunnel integrity?	At what times will employees need to access the network? All at once?	What are the costs of outsourcing?
Are there enough employees with knowledge of VPNs to staff a help desk and configure clients with VPN software?	How will the network need to be restructured (i.e. the firewall, dmz)?	Are there any hidden costs?

Answering these simple questions can clarify what it will take to implement a VPN and whether it is a feasible option. A company may already be using a virtual private network to allow business partners to access certain applications on their networks. If this is the case, they may already have the expertise and infrastructure to support remote access for their own employees.

VPN Security

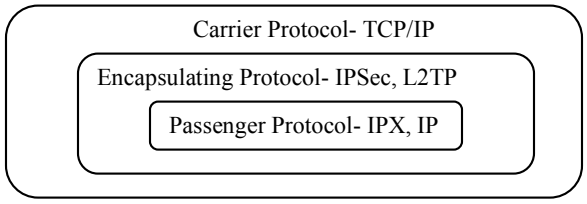
Before users can even access their internal network from home, they must somehow communicate to the server who they are and provide unique information that tells the server that they should be allowed to have access to the network. However, determining how users will connect and how they will be authenticated can be a daunting task, since there are so many options, and ultimately, the security administrator is the one that will be looked at if there is a security breach. Therefore, these options need to be thoroughly researched and considered. A VPN provides a secure way to provide access, without installing expensive, dedicated lines.

"A VPN is a way of wrapping the data packets you pass back and forth between your PC and your employer's servers in a web of data encryption—encryption so strong that shipping those precious packets out over the Wild and Woolly Web is perfectly safe. VPNs assume that there's a packet snoop lurking behind every node, and they are determined to stop your information from being observed en route by such Bad Guys."[2] Many network administrators are implementing this secure method over other alternatives, such as dial-up or leased lines. Of course, the greatest advantage to using a VPN is security. Why is a VPN so secure? As referenced in the above quote, VPNs provide reliable data encryption between two sites over the public Internet. When a protocol that is unrecognizable to the Internet is being sent, this protocol is encapsulated in another protocol such as IPSec or L2TP which travels over a network that uses TCP/IP. Upon reaching its destination, it is evaluated for authenticity and

[2] Seymour, 1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

integrity, and the data is removed from encapsulation.[3] The diagram below depicts what is occurring:



Source for information in diagram: Mairs, 217.

Tunneling

There are two ways tunnels can be created. The first is a client-initiated tunnel in which the tunnel is created from the remote user to the corporate network. In this scenario, the client must have protocol software installed on their remote PC. This presents some added difficulties for the IT department. First, there will be increased support costs for users because users will have to maintain this software on their computer. Within a small company, this may not be an impossible task, but within a larger organization, the problems could mount, especially if employees are using their home PCs, rather than company issued laptops. First the software will have to be installed and configured on each PC. And if anyone has experience with help desks, they know that the first time a user attempts to connect, there will be problems. This means increased calls to the help desk which equates to increased costs. The other option is to use Network Access Server-Initiated VPNs. In this situation, a company institutes an agreement with an Internet Service Provider whereby all of the remote users will dial in to the ISP and it will be the ISP's responsibility to establish a tunnel to the corporate network. Remote PCs do not have to have any special software installed. However, the connection between the remote PC and the ISP is not encrypted, which does create some liability, although it is minimal, considering it is a PSTN (Public Switched Telephone Network) connection, rather than an Internet connection.[4] Choosing between the two options is difficult. A chief factor in determining the right choice should be how much the company can rely on the employee's technology knowledge to successfully connect. In some situations, the client-initiated tunnel may be the best option if management is extremely concerned about security since the unencrypted portion of the connection is removed. However, if management is more concerned with making connections as simple as possible for employees, then the best route is the NAS-initiated option.

Encryption & Authentication

There are several protocols that can be used for encapsulation. The main protocols are PPTP (Point-to-Point Tunneling Protocol), L2TP, and IPSec.

[3] Mairs, 209.
[4] Mairs, 230.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

PPTP: PPTP uses PPP (Point-to-Point Protocol) to encrypt data into IP datagrams. These datagrams are transported by the PPTP to their destination. The PPP protocol is also used for authentication, but does not provide tunnel authentication, which means the actual packets forming the tunnel are not "cryptographically protected".[5] Therefore, this method provides less security than IPSec which is discussed below. Authentication options include, but are not limited to:

- **MS-CHAP:** Microsoft Challenge Handshake Authentication Protocol uses a challenge-response mechanism with one-way encryption on the response.[6] MS-CHAP v2 is the new version of MS-CHAP and it provides stronger initial data encryption keys and different encryption keys for sending and receiving.
- **CHAP:** Challenge Handshake Authentication Protocol uses Message Digest 5 which is a standard hashing scheme. This process converts data so that it cannot be changed back to the original form. [7] The challenge-response method allows the user to be authenticated, without actually sending the password over the connection.
- **Password Authentication Protocol:** PAP uses plain text passwords, and is therefore, less secure. The user is authenticated only at the beginning of the session, whereas with CHAP, the user can be repeatedly challenged for identification.

One advantage to PPTP is that all computers with the Windows Operating System already have the protocol software installed. When considering how to connect users to your network, this could save both time and money because there will be no need to install additional software on each user's computer.

***IPSec and L2TP*:** IPSec is a compilation of security protocols that separate network traffic virtually using tunneling and encryption protocols to make the data invisible to others. The IPSec architecture is comprised of three main components, including the authentication header protocol, the encapsulating security payload protocol, and the Internet key exchange protocol. The authentication header protocol verifies both the identity of the transmitter of the data and that the data has not been tampered with. The encapsulating security payload protocol has both authentication and encryption functions and can be used in conjunction with the authentication header protocol. The Internet key exchange protocol is a negotiation protocol that allows users to agree on authentication methods, encryption methods and the keys to use.[8] Within IPSec, there are two types of modes, the transport mode and the tunnel mode. The Tunnel Mode is more secure because it encapsulates the entire packet,

[5] Mairs, 259.
[6] Microsoft
[7] Lisenbardt & Stigler, 143.
[8] Mairs, 381.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

whereas in the Transport Mode, only the data part of the packet is encapsulated. The Tunnel Mode is normally used when connecting two LANs and the Transport Mode is used when two computers are connecting.[9] Before a packet is sent, IPSec performs the necessary encryption negotiation and authentication. IPSec is often used in conjunction with L2TP because L2TP allows the tunneling of non-IP protocols across the Internet. On the other side, with IPSec, the transport protocol is protected, whereas in L2TP, it is not.

Encryption is used to ensure that packets are protected from hackers' prying eyes. Before encrypting the data, however, appropriate authentication must occur. A useful authentication protocol that provides functionality for more secure user authentication is the Extensible Authentication Protocol:

- **Extensible Authentication Protocol (EAP):** As security becomes more difficult to maintain, network administrators will increasingly turn to alternative methods of authenticating their users to the company network. Because EAP protects against password guessing by dictionary and other types of brute force attacks, EAP is critical in the security of VPNs[10]. In addition, EAP is versatile in that it provides authentication services for token cards, Kerberos V5 protocol, smart cards, and biometrics. While these methods do not appear to be as common in the United States, there is a larger use overseas. According to a study conducted by the IDC, token and smart cards were a $314.5 million dollar market in 2000 and will reach $2.2 billion in 2005.[11] These alternative methods are detailed below:

  - **Token/Smart Cards:** Token and smart cards increase the level of security by requiring two pieces of unique information for authentication. Security is further increased by requiring that the second piece of information be randomly generated every 60 seconds. This code, in addition to the unique PIN already assigned to the user, must be validated by the server before access can be granted. Furthermore, since the user only has to remember a PIN that is not changed every 60 days as passwords often are, the chances of the user forgetting their PIN are significantly less than when they must remember a 6-8 alphanumeric password. "According to industry estimates, up to 30% of support calls are about lost passwords, and manual password resets cost between $15 and $30 per call"[12]. However, while token cards provide enhanced security, as with anything, they are not infallible. While a common Login ID/Password scheme forces users to retain password information in their memory, users must also retain their token card and protect them from destruction and loss. And considering the human beings capacity for losing things (personally, I have lost my

[9] Cope, 1.
[10] Microsoft, 1.
[11] Radcliff, p. 1.
[12] Gilhooly, p. 1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

security pass card 4 times since I started my job 2 years ago), the costs of replacing cards when lost may outweigh the cost of resetting passwords.

- **Biometrics:** EAP also supports Biometric authentication. Biometrics stores unique physical information, such as a person's fingerprint or iris pattern to validate a person's authentication attempt. Biometrics is advantageous because users do not have to remember a password. While this method is not widespread currently, there is potential for it to become increasing popular as companies look for more secure ways to identify their users.

In brief, two main considerations in implementing a VPN include whether to use a client-initiated tunnel or a network access server-initiated tunnel; which protocol will be used, and what authentication method will be used.

Monitoring Remote Access

Once remote access is implemented, the IT department must continuously monitor access to identify potential break-ins and uncover unauthorized activity, including activity by those users that have the right to access the network. Two key components in maintaining a network are a firewall, which is essential in any network that is connected to the Internet, and an intrusion detection system which can go one step beyond the firewall and monitor all network activity, not just monitor the perimeter of the network. In addition, the intrusion detection system will analyze the patterns in network traffic and reveal any irregularities that may actual be inappropriate behavior.[13] An intrusion detection system can send emails or pages when there is a possible security breach. Even if the company is not implementing remote access, an intrusion detection system can be a valuable resource in stopping an attack. Equally important is the knowledge of how to handle an attack. The IT department should have documented procedures for handling security breaches. In addition to monitoring outside activity, the internal IT department should periodically attempt to find weaknesses in their own network. Employing hacker mentality could be the key to reducing threats of malicious activity. Existing weaknesses should also be identified and if they can't be resolved without a large expense, at least ascertain how the weakness could possibly be exploited and determine if the incident can be stopped before significant damage is caused.

In addition, system performance must also be monitored to analyze traffic patterns and ensure that the company's network can handle VPN connections. Performance, especially when implementing IPSec can be significantly reduced once the number of connections increases significantly. Monitoring traffic will allow the IT department to evaluate the need for expanding capacity.

[13] Mairs, p. 161

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Remote Access Policies

Once these decisions have been made, the network administrator will embark on one of the crucial areas of providing remote access to employees. It is very important to continuously monitor remote access and implement policies that will protect the company's resources. Remote Access Policies can refer to two different concepts. First, companies should define policies on their servers that set limits on access. For example, administrators can define settings that delineate when a user can access the server, or in dial-up cases, the originating phone number can be set. If the user attempts to dial in from a phone number different from the one in the policy, the user will be denied access. The IT manager could also consider setting up maximum connection times. For VPNs, using Window 2000 Remote Access Service, administrators specify which connections can be granted permission, based on the tunneling protocol they use. Windows 2000 server also provides VPN and dial-up support on the same server. In other words, the administrator can specify encryption to be used for a VPN connection and not for a dial-up connection.[14] The remote access server can also be set to disconnect from the user immediately after the connection is established. The server then calls the user back at a pre-specified phone number.

Remote Access Policy can also refer to a document that defines the responsibilities of both the employer and the employee related to remote access. Policies such as these not only clearly define responsibilities, but they may also serve as some protection to the company in the event that the employee performs malicious activity while using the remote access service. Elements of a comprehensive remote access policy include:

- *Role of the IT department in supporting employees using remote access:* The IT department must be able to provide support for maintaining the network so that users can connect with minimal problems and minimal downtime.
- *Role of the employee in safeguarding their password or other authentication mechanisms such as token cards:* Users should notify the IT department immediately if their password is compromised or if their token card is last.
- *Responsibility of the employee to use the remote access for business related purposes only:* The policy should detail what the user is allowed to do once they are connected to the network.
- *Employee understanding of application access:* In addition, users should understand that they will be given access only to those applications and areas that are necessary for their job functions.

[14] Toombs, 4.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- *Responsibility of the employee to notify the IT department if any suspicious activity is noted:* If the user notices anything unusual while accessing the network, the IT department should be notified immediately.

Employees should be required to sign a copy of the policy, stating that they have read and understand the policies and procedures related to remote access. The policy must be enforced, in other words, if an incident occurs, action must be taken. Adding remote access means opening up yet another possible hole in the security of a company's network. Even if remote access is implemented in the most secure manner, there will still be ways to breach security and most often, it will come from inside the company.

The implementation of remote access is a large endeavor with many considerations. First and foremost is establishing a business case that will induce management to provide essential support. In conjunction with this, the IT manager will have to take into account both cost and security issues. Once the decision has been made to provide remote access, the IT manager will have to begin the tedious task of creating an implementation plan. When choosing a VPN solution, two options that should be considered are whether to use a client-initiated tunnel or a network access server-initiated tunnel. In addition, decisions will have to be made regarding which protocols will be put in place and what authentication method will be used. Finally, because the establishment of a VPN increases security concerns, the IT department will need to increase the monitoring of network activity and establish and enforce policies related to remote access.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Sources (Note that some URLs may need to be cut and pasted into the address box)

Brewin, Bob. "Emergency Plan B". Computerworld. January 21, 2002. URL: http://www.computerworld.com/itresources/rcstory/0,4167,STO67549_KEY18,00.html

Cope, James. "Outsourcing VPNs: Privacy for Hire". Computerworld. February 11, 2002. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO68069,00.html

Cope, James. "IPSec: Making the VPN Secure". Computerworld. February 11, 2002. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO68070,00.html

Gilhooly, Kym. "Smart Cards, Smart Move?" Computerworld. 21 May 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO60688,00.html

Lisenbardt, Mark A. and Stigler, Shane. "Windows 2000 Administrator's Handbook". Foster City: M&T Books, 2000.

Mairs, John. "VPNs, A Beginners Guide". Berkeley: McGraw-Hill/Osborne, 2002.

Microsoft. "Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)" February 28, 2000. URL: http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/auth_mschapv2.htm

Microsoft. "Extensible Authentication Protocol". MSDN Library. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/eap/eapport_0fj9.asp

Microsoft. "Windows 2000 Server Documentation". URL: http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_rap_intro.htm

Radcliff, Deborah. "Beyond Passwords". Computerworld. January 21, 2002. URL: http://www.computerworld.com/itresources/rcstory/0,4167,STO67551_KEY18,00.html

Seymour, Jim. "The Hidden Truth about VPNs". PC Magazine. July 1, 2001. URL: http://www.pcmag.com/article/0,2997,s=1502&a=4792,00.asp

Toombs, Douglas. "Creating Remote Access Policies". Windows 2000 Magazine. October, 2000. URL: http://www.win2000mag.com/Articles/Print.cfm?ArticleID=15489

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.