Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2e

Submitted by: Michael A. Wilson

Keeping the Private Intranet Private

In today's interconnected world, a company's private network, the intranet, often is not so private as it once was. Inter-company relationships and employee connectivity needs often require other computers to be able to connect to the intranet through an uncontrolled network. (For the purposes of this discussion even a dedicated connection such as a T-1 line is considered uncontrolled.) How can an administrator of the intranet have a reasonable confidence that these communications lines are not being used for unauthorized access to company data?

Between employees working from home or on the road, customers needing access to data, and vendors who may be accessing data or updating systems, there can be many points of access to a corporate intranet. Each one of these points is a potential security hole that unauthorized people can use to access the private data of the corporation. The problem faced by network administrators is how to control those access points and minimize the risk involved.

International Data Corp. performed some market research that indicated that there will be more than 20 million broadband users in the United States by 2003. Of those users, sixty-four percent plan to access their corporate network remotely over these high-speed connections[1]. Craig LaHote, network administrator at SR Equipment, admitted that remote access is hard to control. He stated that "we really have a hard time enforcing policies there. We have a policy but no real way to audit [users] except basically asking them to comply."[2]

One of the more popular methods of controlling access to the intranet is the Virtual Private Network (VPN). A VPN encrypts data between two points so that anything passing between those two points cannot be understood by somebody eavesdropping on the communication. In this way, it assures that the data is protected from unauthorized viewing or tampering as it traverses the Internet.

A VPN can be configured between two networks, or between a single computer and a network. A VPN between a single computer and a network works well for connecting employees who are working from home or on the road. In this scenario data is encrypted at the employee's computer and unencrypted at the border of the corporate intranet. As the data travels across the Internet, it cannot be viewed by someone else.

VPNs also work well for connecting business partners across the Internet. A VPN can be set up

between the respective intranets so that all communication between the networks is encrypted. An example is an individual in one company needing to send information via FTP to another company. FTP is an inherently insecure file transfer method since the user id and password are sent across the network in plain text. However, if a VPN is established first, the user id and password are encrypted by the VPN before being sent over the public network.

The VPN, however, is not a magic blanket solving all of the problems of connecting remote users to the intranet. There are several issues that a VPN does not address. Basically, a VPN extends the intranet beyond the firewall by allowing a computer or network outside of the firewall direct access to the intranet. However, the VPN itself does nothing to protect the remote computers and networks at the other end of the connection. If access to these remote systems is not protected, then that severely degrades the effectiveness of any other protection measures that are in place. As Mike Hager, vice president of security at Oppenheimer Funds, stated for InternetWeek, a company's overall security "is only as good as the home PC security."[3]

As an example, take the case of an employee connecting to the corporate network from home. This individual has a DSL connection to the Internet and uses a VPN to connect to the company's intranet. The VPN does nothing to protect the employee's computer at home or prevent a hacker from gaining control of it. Once a hacker has this access, they can view any data that is on the home computer, or can use the VPN to access the corporate intranet. The VPN also provides a clear path into the intranet for any trojan horse program that may be on the user's computer, or for e-mail messages with dangerous attachments. This same scenario can exist with a VPN between business partners if someone gains unauthorized access to a business partner's network or if their network is not secure against trojan horses or viruses.

A defense-in-depth procedure needs to be followed outside of the company's intranet as well as inside. A defense-in-depth approach to security creates multiple levels of protection. A firewall alone is not enough to protect the intranet. Nor is a policy for strong passwords. Both of these methods for protecting the intranet should be used in addition to others. Using a defense-in-depth approach provides greater protection because if someone finds a way to bypass one level of security, there will still be other levels protecting the intranet. This method of securing the network should be applied not only to the intranet and computers residing inside the corporate network, but also to any computer connecting in from outside the intranet.

In the case of an employee connecting from home there are a couple of different approaches that can be taken. First, a company could require that current anti-virus software and a personal firewall exist on an employee's home computer before granting access to the intranet. However, this solution has problems of its own. In the case of a non-technical employee, who is going to make sure that the software is configured properly? Also, how can the company be sure that the software is not only configured properly, but is active? Finally, if the company is dictating what software should be installed and configured, then they are opening themselves up to support calls when those applications break other applications that are already on the user's home computer. In that case, an already overworked IT department now has the additional job of supporting the home computers of anyone who connects to the intranet.

The second approach is more expensive, but could be considered more secure. In this case, the company provides a computer to an employee who requires remote access. This computer would be given to the employee with the understanding that it is for business use only and no other software should be installed on it. The computer would have to have appropriate security installed on it so that, regardless of whether or not it was being connected to the intranet, the computer would be relatively secure. The computer would need to be running Windows NT or Windows 2000 so that the operating system could be configured to prevent the user from installing other software. It would also have appropriate anti-virus software and personal firewall software installed. In order to keep maintenance of these remote systems from becoming too difficult, the anti-virus software and personal firewall would need to be manageable from a central location.

While VPNs, anti-virus software, and desktop firewalls have been around for a while, getting them to work together as a cohesive system has been difficult at best. Recently Linksys, Zone Labs, and Trend Micro took a step in this direction by forming a partnership to allow their products to work together. The partnership uses Linksys' NAT-based router, Zone Labs' ZoneAlarm Pro personal firewall, and Trend Micro's PC-cillin anti-virus software. The key to this configuration is the LinkSys router. This router checks the client PC to be sure that it has the proper policies and security measures in place. If these policies are not in place, the user is directed to a web site where ZoneAlarm Pro and PC-cillin are available to be downloaded. Steve Janss reviewed this setup for Network World and noticed only a small decrease in performance when the system was under attack[4]. One drawback to this approach from a corporate point of view is that, since a Linksys router is required on the home network, the company is dictating the configuration of the employee's home network. This could require the company's IS staff to support the employee's network.

Another comprehensive product is Sygate Secure Enterprise developed by Sygate Technologies Inc. This product uses a Management Server, a Security Agent, and a VPN Enforcer. The Security Agent resides on the end-users' PC. It enforces rule-based security that combines intrusion detection capabilities with an application-centric firewall. Additionally, the Security Agent can be configured so that there is no icon in the system tray and no entry in the Programs menu, which makes the Security Agent invisible to the user. This prevents them from making changes to the rules and policies. The Management Server runs on a Microsoft IIS server and provides administrators with a central point of control over the Security Agents. Using the Management Server, administrators can define, deploy, monitor and enforce the security policies. Rules can be created based upon user, computer, application, port, protocol, time, host, location, or adapter. The final piece of this product, the VPN Enforcer, ensures that the user connecting through the VPN is running the Sygate Security Agent and has the proper policies installed before allowing access to the corporate intranet. The VPN Enforcer sits behind the firewall and acts as an IP Forwarder between the VPN and the rest of the intranet. There is a drawback to this product though in that there is no anti-virus solution incorporated in this package, although Sygate is looking to add this functionality in a future release. While it would be possible to use a separate anti-virus product, the VPN Enforcer would not check to be sure that the anti-virus was active and up to date.

Employees are not the only people needing access to the corporate intranet. Business partners often need access to view data or update systems. When working with an employee's connection to the intranet, it is possible to dictate how the remote computer is configured, and what software needs to be running on it in before allowing a connection to the intranet, especially if that computer is company-owned. When working with a business partner, a company often does not have this level of control. A company cannot require the business partner to run a particular anti-virus package, or personal firewall on their desktops. There are, however, some steps that can be taken to protect the intranet.

When connecting to a business partner via a VPN configuration, determine where the end point of the VPN is going to be in the partner's network. Ensure that the VPN terminates in a secure portion of the network where access to the network is restricted. Does the VPN terminate in a DMZ area of the network that is dedicated to your company, or does it terminate in area of the network that is accessible to anyone in the partner's network? A point to keep in mind when determining this information is that not everybody in the partner's network may need access to the intranet.

While it is not reasonable to demand that a business partner be using a particular application in their systems, it is reasonable to require that they are using a particular type of application. For example, while it is not reasonable to require a company to be using McAffee anti-virus software, it is reasonable to require that they be using some form of anti-virus software and that it is kept up-to-date.

One of the ways to determine the security level of a business partner's network is to find out what security policies they have in place. How do they control access to their network? Do they have firewalls in place that are properly configured? Are they keeping their anti-virus software up-to-date? Are they scanning e-mails? Are they doing content filtering on the web pages that their employees are viewing? How are they controlling remote access to their network? The problem in this situation is that the business partner may not be willing to provide that information. Their argument may be that if they give out detailed information about their network security, it could be used by someone to access their intranet without authorization. However, the information does not have to go into detail about which products they use. General information on the fact that access is controlled, and whether or not it is audited and monitored may be all that is needed. The level of detail that is required depends upon the level of access to the intranet that is going to be required by the business partner. If a partner is sending you a file on a daily basis via FTP, it may not be necessary to know some of the above information. However, if they are being granted telnet access to a unix host, you want to be confident that there are not any unauthorized users roaming through their network looking for a way into yours.

This information needs to be determined before the partnership is formed. After the partnership is in place and work has begun, it is often too late to find out that your partner does not have any anti-virus protection. Finding out that your partner does not have any anti-virus software by tracing a virus infection back to their network can institute a level of distrust between the companies which can hamper the accomplishment of the business goals which the partnership was set up to achieve. In order to prevent this situation from occurring, upper management

needs to be aware of the security issues involved so that they may deal with them while the partnership is being developed. Also, there may be instances where the business partner's network does not have the level of security that you normally require, but it is necessary to link the networks anyway because of business requirements. Management needs to make the security administrators aware of this so that a higher level of auditing can be done to attempt to compensate for that weakness. In an ideal situation, business partners would have periodic security audits performed and would be willing to provide a summary of the information gained in these audits.

Once physical access is under control, another issue that needs to be considered is what happens to information after it leaves your intranet. If an employee is traveling and accessing the corporate intranet, what are they doing with the information they are retrieving? If they are printing to a printer in a hotel business center, how long do they leave the papers sitting on the printer before they retrieve them? If they are working in a public area, who is able to look over their shoulder to see that information? For instance, an airport waiting area may not be an appropriate place to be working on a highly confidential document. These are issues that cannot be controlled directly by the administrator. They can only be dealt with by educating the user and helping them to realize the importance of what they are working on in relation to their surroundings. Also, if the user feels some ownership responsibility for the data, then they are more likely to safeguard that data. Fred Rica, a partner in the technology risk services practice at PriceWaterhouseCoopers, was speaking to this topic when he stated that "technology will solve less than half this problem. The other portion is working with people's behaviors."[5]

Similar confidentiality issues exist in working with business partners. Since information is being shared between companies, it is logical to assume that the employees in the partner company will have information displayed on their computer screens or on print-outs laying on their desks that your company considers to be of a confidential nature. Since the two companies are working in partnership together, there should be a reasonable level of trust in the partner's employees. However, what other partners does that company have? If they are partnered with a competitor of your company, will the competitors employees gain access to the confidential data through the mutual partner? Once information leaves your company's control, it cannot be retrieved and it becomes almost impossible to regain that control.

As an example, consider the following scenario. Your company partners with an application development company, Xpert Developers, to create a custom information retrieval application so that your customers may retrieve information from databases residing in your intranet. In order to maintain the application once it is in production, Xpert Developers is granted access to the application servers on the intranet so that they can update the software. You also have access into Xpert Developers network in order to test updates to the application. Unknown to you, Xpert Developers is also doing some development work for one of your major competitors and has a similar relationship with them. In meetings between Xpert Developers and your competitor, employees of your competitor see a name and password for access to your intranet. Once back in their own offices, your competitor links into the Xpert Developers network and then, using the name and password they discovered, connect to your intranet. A major competitor now has the same access to your network as someone you consider to be a trusted

partner.

There are a number of other issues involved in maintaining security on computers and networks that are connecting from outside of the intranet. Unfortunately many of those issues do not have solutions in today's environment. How do you enforce strong passwords on an automated process that transfers files into your network? How do you allow an ftp user to change their password securely? Network and security administrators continue to deal with these and other issues.

The more dynamic your business is, and the more connections that are allowed from external computers and networks, the more difficult it becomes to secure the perimeter of the intranet. In today's inter-connected world, that perimeter is now flexible and always in a state of change. Many organizations take a defense-in-depth approach to securing their intranets. They have firewalls in place. They use two-factor authentication. They have anti-virus software running on their desktops, and they do content filtering when browsing the Internet. However, it can be easy to overlook the connections that extend your intranet into unsecured locations. Security professionals must always be alert to the avenues of access into the intranet and be sure that defense-in-depth is extended to wherever your intranet is extended. A VPN does not automatically ensure that your network is protected. Systems and policies must be in place to protect the computers and networks at the far end of the VPN as well.

References:

[1] Yasin, Rutrell. "Telecommuters On Security Alert." InternetWeek. 3 May 2000. URL: http://www.internetwk.com/story/INW20000503S0001 (6 October 2001).

[2] Berinato, Scott. "Teleworkers bring thorny problems to security's front lines." 17 November 2000. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2655595,00.html (6 October 2001).

[3] Yasin, Rutrell. "Telecommuters On Security Alert." InternetWeek. 3 May 2000. URL: http://www.internetwk.com/story/INW20000503S0001 (6 October 2001).

[4] Janss, Steve. "Triple your remote protection." Network World. 6 August 2001. URL: http://www.nwfusion.com/net.worker/news/2001/0806networkerreview.html (28 September 2001).

[5] Berinato, Scott. "Teleworkers bring thorny problems to security's front lines." 17 November 2000. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2655595,00.html (6 October 2001).

Costello, Sam. "Sygate looks to secure remote workers with new software." Network World Fusion. 15 June 2001. URL: http://www.nwfusion.com/news/2001/0615sygate.html (28 September 2001).

Sygate Secure Enterprise Product literature
URL: http://www.sygate.com/products/sms_ov.htm

Gittlen, Sandra. "VPN security requirements debated." Network World Fusion. 17 September 2001. URL: http://www.nwfusion.com/columnists/2001/0917gittlen.html (20 September 2001).

Collin, Barry C. "Extranet security: What happens if your partner turns against you." Computer Security Alert. October 1997. URL: http://www.gocsi.com/extranet.htm (8 September 2001).

Last Updated: July 26th, 2017

Upcoming Training

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 New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS