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

Security Concerns and the Use of Microsoft Virtual Private Network for Small Businesses

By Teresa Hummel
GSEC Option 1
Assignment Version 1.4b

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract

This paper will cover Microsoft Virtual Private Network (VPN) service and steps that should be taken prior to setup. Emphasis will be on Windows 2000 as the operating system for the VPN services. It will look at the types of connections a small business might expect to encounter when using VPN's. The security concerns of choices in the set up of the connections for both parties including: type of encryption available and Firewall issues. Last of all what are the overall security concerns when using Microsoft VPN including past problems with a discussion of fixes and security patches.

Security Concerns and the Use of Microsoft VPN for Small Businesses

Small businesses often operate on a tight budget; recently VPN's have become a very cost effective way for them to connect from home, on the road, and with other offices. Prior to VPN's the favored ways to securely connect to the office network were through direct dial-in and leased line connection, both options could be extremely costly to the company in terms of dollars.

VPN's allow access through an internet connection. This connection can be established through a local call to an ISP, a DSL line, or cable internet connection. When set up and configured correctly, the cost to connect is very low, connections can be robust, and the security is excellent. For the purposes of this paper "server" will be defined as the VPN server of the home office network and "client" will be the remote site requesting a VPN connection.

Microsoft's VPN services are very easy to set up and monitor, especially for small businesses where limited connections will occur. Microsoft has excellent documentation available for helping to set up VPN services with Windows 2000. [Ref. 1] It is worthwhile to note that Microsoft sets the minimum requirements for a Windows 2000 VPN server: Pentium 133 or higher processor, 128 MB RAM (256 MB recommended), and 4 GB HD [Ref. 2]. More RAM, a faster processor, even more available servers allowing a VPN connection, will accelerate throughput and avoid slowdowns. This can be important because inadequate hardware may cause the mistaken impression that the encrypting process used by a VPN slows down the exchange of information.

Before installing the VPN services, however, a number of things must be taken into consideration. By evaluating who is using the VPN, the hardware necessary to make good connections, the pros and cons of differing connection protocols, and evaluating past security problems, setting up the VPN services becomes a much smoother process.

David Aylesworth [Ref. 3] asks the following questions:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Are you connecting multiple offices with the VPN (site-to-site)?
- Are they company offices (intranet) or business partners (extranet)?
- Are you connecting remote users to the VPN (remote access)?
- If yes, are they company employees (intranet) or customers (extranet)?

Let's start with the first question. It's becoming more common for small businesses to work in a very decentralized manner. This might be the case when there is a central office with some of the employees working from home, or a central office with several branch offices. Whatever the arrangement, the need is for these networks to securely communicate with each other. This is known as site-to-site communication. The number of connections being made, the amount of data being transferred, whether or not a persistent connection is needed, all play a role in the way the VPN services are set up.

Next there is a need to look at who is accessing the VPN. Employee communications will have different internal security concerns from outside business partners. With company employees, the need is to allow them the same access they have when they are on the premises. Business partners may need access to the company intranet, however it may be possible to create a set up that is separated from regular company resources. Allowing just the access that is necessary to conduct business, and no more, is the safest method for everyone.

Remote connections, generally sales people out on calls or company employees traveling on business pose yet another type of security concern when setting up a VPN. These are single machines from varying locations, having periodic access to the company network behind the firewall.

VPN's and Firewalls

Anyone who will be accessing the VPN services should have a firewall in place. Once a VPN connection is established, the client is essentially able to access information behind the company's firewall, thus creating an access hole. Therefore, insisting a client use and maintain a firewall is another layer in the security of the VPN setup.

The ease of changing the firewall rules to allow VPN connections should be addressed. Very old firewalls, either appliance types or software types, may be difficult or impossible to configure to allow VPN access. A small business may stay with an old firewall for many reasons, one of which might be the fact that there has been no reason to upgrade in the past. It would be prudent to check the firewall documentation before becoming enmeshed in the VPN process, only to have it fail for lack of access, or creating a setup that might be considered insecure.

Site-to-site connections should have a firewall at each end of the connection. If the firewalls are in front of the VPN servers, they will need to be configured to allow the VPN packets to pass through directly to the VPN server. One or more servers at each end of the connection can be set up to handle the VPN traffic. All VPN traffic can then flow

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

through these portals. By using routing tables, only this type of traffic need flow through the VPN, other traffic, such as browsing, can use a direct route to it's destination.

For remote connections, insisting on a policy of the client having a personal firewall in place is a good idea. It's easy to allow VPN traffic through a personal firewall, and the machine will be protected when accessing the network without using the VPN. It is possible, and could be considered good practice, to set the machine to connect to the internet using the VPN services. Therefore, when dialing out and connecting, the remote client is immediately connected to the server. All activities are then conducted behind the office firewall. This will lessen the chance that an attacker can access the client machine and use the VPN connection for accessing the intranet behind the home base firewall.

Once the client is connected to the intranet via the VPN, they must be considered to be like any other machine in the network. Any Trojan or virus on the client machine now has access to the intranet too. Therefore, networks that allow VPN connections have yet another reason to keep tight security on all machines to prevent problems.

User Considerations

When setting up the VPN server(s) at the main office, who is using the connection and how much access to the internal network, need to be considered. Employees usually need and want the same type of access they have in their own offices. Access to email, applications, mainframe computers; all can be accomplished with a good VPN connection. One possibility is to direct the VPN connection to a server that allows the employee to start a terminal services session. From this session, the employee would be able to work in exactly the same manner as being in the office with exactly the same privileges. Since terminal services allow the user to logon and logoff without losing session information, it's a valuable tool to use in conjunction with a VPN connection.

For business partners who need a VPN connection, thought must be given to how much access is acceptable. Best practice would be to set up VPN servers for those outside the company in a DMZ type area with a firewall between them and the company network. These would work along the lines of an email server. For example the business partner uses the VPN, uploads data to a holding area, a company employee then accesses the data and downloads it to the company side. In this way there is never any direct access to the company network by outsiders and conversely the business partner need not expose their own system to another company. This may not be an option in some cases. If it is necessary to allow outsiders access to the intranet, strict access controls are necessary, possibly by using a second firewall in back of the VPN server to restrict access to certain areas.

The Protocol Set Up

Now that we have looked at who will be accessing the VPN, the hardware necessary, and the use of firewalls, the next area to look into is the VPN server itself. What is involved in the setup and what security considerations are necessary?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Passwords and pass phrases should be taken into account from the very beginning. Some setups of the VPN will require passwords or pass phrases. These should follow the usual standards of using numbers, upper and lower case letters, and special characters to make them difficult to crack. Since passwords and phrases are entered and saved during the VPN setup, the problem of remembering them each time the VPN negotiates a connection, is not an issue. Small businesses will find it easier than large businesses to directly communicate passwords either on the phone or face to face. If email is used, it should be encrypted to ensure integrity.

Microsoft has 2 types of protocols available to connect a VPN client with a VPN server. These are Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2PT)/IPSec. PPTP and L2TP are both layer 2 protocols in the Open Systems Interconnection (OSI) Model. Layer 2 is the data-link layer. IPSec is a layer 3 protocol; this corresponds to the network layer in the OSI Model. "A Tunnel is the portion of the connection in which your data is encapsulated. (Data that is tunneled must also be encrypted to be a VPN connection)". [Ref 4] To better make a decision about which protocol to use, it's best to understand how each works, the amount of security provided, and the difficulty of maintaining the protocol.

PPP or Point-to-Point Protocol is the basis for PPTP and L2TP. It was originally developed for dialup connections and has been supported and modified over the years; keeping it current and enabling it's use in other types of internet connections. There are 5 main features of PPP [Ref 11]:

- Address notification: which, among other things allows the server to notify the client of its IP address and enables clients to request an IP address
- User authentication: authentication is accomplished using Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), and MS-CHAP version 2
- Extensible authentication protocol (EAP): enabling the server to determine the type of authentication protocol used
- Multiple protocols: support for these various network environments TCP/IP, IPX, and NetBEUI
- Link monitoring: continuously monitors the state of the link.

To create the PPTP link, PPP is used to connect to the internet and authenticate the user, then PPTP creates a connection to the server, last of all the PPP packets are encrypted and encapsulated (or tunneled) to securely send data over the connection. TCP is used to transport these packets along with a second TCP connection that carries maintenance data. Since, the entire packet of original data is encapsulated, it is possible to run remote

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

applications that require specific network headers. PPTP data encryption begins after the PPP connection process and before PPP authentication is completed. This is user level authentication only. [Ref 5] Earlier versions of PPTP that run on older Microsoft operating systems need to be patched. This will be discussed later.

L2PT/IPSec takes the features of PPTP, Layer 2 Forwarding (L2F, created by Cisco), and combines them with the security of an IPSec connection. This protocol started out as an IETF standard and is defined in RFC 2261. [Ref 12] This means as time goes on more companies will support this standard as opposed to a proprietary protocol. Since this is a standardized protocol, it also works with third party vendor products. The setup of L2TP/IPSec is more involved, but once this is done, the operation, from outward appearances, looks exactly the same as a PPTP connection.

Instead of TCP, L2TP frames are transported in UDP packets. Unlike PPTP, which requires a second TCP connection for maintenance, L2TP uses UDP packets over the existing connection. The PPP packets carrying the information can be encrypted, compressed, or both. L2TP has nothing to do with the actual encryption of the information. Encryption is accomplished using IPSec.

IP Security or IPSec is the protocol used to give authentication or encryption to IP packets, often using computer certificates. The connection is computer level authentication. This is the standard method used and is another level of security for data in the VPN stream. It is possible to configure the connection using a shared key instead of certificates. This might be done if the client is connecting from a foreign country. Higher-level encryption cannot be exported; therefore a shared key structure would need to be used.

Although L2PT is more secure, it may not be supported on all client platforms. There is the added work of using certificates to authenticate the connection. For small businesses it may be a fairly easy matter to set up an in-house Certificate Authority. If there are only a few VPN connections to maintain, keeping track of certificates is less complicated.

The requirements to install Certificate Authority on Windows 2000 are fairly straightforward. Because certificates are based on timestamps, it's necessary to make sure the date and time are correct on the server. Certificate Services can be added through the Add/Remove Window. There is a step-by-step walk through of Certificate Authority setup on ZDNet. [Ref 10]

Network Address Translation (NAT) cannot be used with L2TP/IPSec and is one of the major drawbacks when using this method. Internet Key Exchange (IKE), the protocol used to negotiate Server Associations, and IPSec protected traffic are not translatable by NAT. [Ref 5] The UDP port number is encrypted and protected with a checksum. Because NAT cannot be used, the IP addresses on both ends of the connection must be static. This can cause major problems with remote dial-in connections. If the employee is on the road, and dials in through a local ISP, the IP address won't be known until after the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

connection occurs. This means a direct dial-in, using the VPN to make the connection, is impossible. There is work in progress for a change in future releases.

Type of Connection

Once the protocol for communication is decided, the next thing to consider is whether or not to use a persistent connection to the VPN server. A temporary connection is useful when VPN servers are at a premium, if the connection is a dial-in, or if there is little traffic between the 2 VPN sites. The VPN connection can be established and then can disconnect on it's own if no data is being sent. The time limits for this can be modified with the default being 20 minutes.

A persistent connection can be set up for those who need a continuous connection over the VPN. This should be used over a DSL or Cable line where the client has a continuous internet connection. If the connection is lost, there is automatically an attempt to reconnect.

Earlier it was noted that VPN services should be used in conjunction with a firewall. There are 2 different ways to set this up. VPN servers may reside in front of a firewall. This is not the usual setup as it leaves the VPN server open to all traffic from the internet. If this is the preferred method, then the server must be locked down tightly with all security patches in place and closely monitored to be sure it hasn't been compromised. With this method packet filters must be employed to route the VPN traffic through the server for authentication. All other packets are passed on to the firewall. The advantage to this setup is that the firewall can be used to allow VPN clients access only to certain parts of the intranet.

More often the setup is with the VPN server behind the firewall in the DMZ with FTP servers and Web servers. The firewall must be set to filter the VPN traffic to the VPN server. In turn, the VPN server authenticates the connection and then passes on the decrypted packets to the intranet.

As it was noted earlier, once a VPN connection is established, the client is basically behind the server's firewall. This means an attacker, to gain access to the server's network, could use the VPN session. Depending upon need, it may be best to confine the VPN connection to the DMZ area.

Security Patches

There have been several significant security events for Microsoft's VPN services.

In 1998 and 1999 Bruce Schneier of Counterpane Labs and Mudge of L0pht Heavy Industries released several papers dealing with security holes in Microsoft's PPTP. [Ref 7]

The original 1998 analysis found many serious flaws in PPTP, at least 5 different areas presented problems. Once again, old unpatched machines setting up VPN services, are

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

vulnerable to multiple types of attacks highlighted as follows: weak algorithms for password hashing, authentication protocol allowing an attacker to masquerade as the server, recovery of encrypted data, breakable keys, and the ability of attackers to crash PPTP servers. Any one of these problems could cost a business in terms of lost data, time, and cleanup if an attacker was able to exploit these vulnerabilities.

Microsoft did release upgraded protocols to fix these vulnerabilities. They upgraded the password hashing, created stronger authentication to prevent masquerading, and prevented password spoofing. Thus the security was made more robust and good enough for many implementations of VPN services. However, if there is concern about very tight security, L2TP/IPSec should be the protocol of choice.

A faulty patch for a security flaw in the Remote Access Service (RAS) was noted in July of 2002. The original patch, issued in June of 2002, for a buffer overrun flaw in the RAS phonebook, caused VPN's to cease functioning. [Ref 6] However, it was later found that VPN's could function, but only using administrative privileges. The bug was reported to NTBugTrac and Microsoft. At the beginning of July, 2002 a new patch was released, essentially taking care of the problem. [Ref 8]

It is entirely possible for older machines to be improperly patched, thus causing a failure of the VPN connection. Users, finding it possible to connect while in the administrator account, will very likely be tempted to login as the administrator, or create another account with administrator privileges to get around the problem. This is always bad security practice, as any account being used should be an account with the least amount of privileges needed to get the job done. The faulty patch was pulled from the Microsoft servers when the bug was discovered and a new patch was quickly released correcting the problem.

In September of 2002 a German company named Phion announced a flaw in the Microsoft PPTP service, a remotely exploitable pre-authentication buffer overflow. "This enables a specially crafted PPTP packet to overwrite kernel memory, such that a denial of service attack can lock up the server." [Ref 9] VPN servers are vulnerable to this attack because the PPTP client is always listening on a port. After evaluating the flaw, Microsoft stated that it could not be used to run arbitrary code on the VPN server.

This is a very serious flaw considering the increasing popularity of VPN's and DSL/Cable connections. The worst problem uncovered so far is the possibility of a denial of service attack. However, any flaw may open up the possibility of attacks from as yet unconsidered directions. Microsoft released a patch in October of 2002. [Ref 12] Anyone considering the use of PPTP should definitely have this patch in place to protect against exploits. The other option is to use L2TP/IPSec which is unaffected by the flaw.

Conclusion

There are many vendors of VPN services available in a wide range of prices. Medium to large companies are the target consumer for most of them. Small companies may wonder

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

if the readily available VPN server of Windows 2000 is up to the task of securing their data properly.

The answer to that must be yes. The VPN server and client are easy to configure. The two protocols available for connections offer clear choices for which ones can be used and the best situations to use them.

This paper is meant to bring up questions that should be answered before a VPN setup is attempted. The planning stage of any operation is the most critical. A poorly planned project wastes time and money for all concerned. It can also create security holes that can be devastating to any company.

Sitting down with all persons involved in the VPN project, looking at all the requirements ahead of time, and finding the answers to all questions possible, will help to ensure a smooth transition to using Microsoft's VPN service.

In a small company, it's even possible to set up one user at a time, get the service running correctly, and move on to the next person. Wide scale deployment may mean only five or six people, or one other network. In this case, the manageability of the VPN service is not difficult and can go hand in hand with usual network monitoring.

Therefore Microsoft VPN services are definitely a "good buy" for a small company.

References:

1. Microsoft Virtual Private Networks
http://www.microsoft.com/windows2000/technologies/communications/vpn/default.asp

2. Microsoft Determining Network Connectivity Strategies
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/deploy/dgcf_inc_lpea.asp

3. Microsoft Configuring a VPN Solution
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/confeat/vpnsol.asp

4. M21 Microsoft Virtual Private Networking
http://www.extra.net/vpn3.html

5. Virtual Private Networking in Windows 2000: An Overview
http://www.microsoft.com/windows2000/docs/VPNoverview.doc 1999

© SANS Institute 2003, Author retains full rights.

6. Computerworld "Microsoft Security fix blocks VPN connections" Joris Evers, IDG News Service July 03, 2002
http://www.computerworld.com/securitytopics/security/holes/story/0,10801,72441,00.html

7. Analysis of Microsoft PPTP Version 2 Bruce Schneier, Counterpane Labs: Mudge, L0pht Heavy Industries 1998-1999
http://www.counterpane.com/pptp.html

8. Microsoft Security Bulletin MS02-029
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-029.asp

9. InfoWorld "Microsoft VPN flaw may open intranets to attack" David Legard September 27, 2002
http://archive.infoworld.com/articles/hn/xml/02/09/27/020927hnmsvpnflaw.xml

10. ZDNet "Configuring the Certification Authority Service" Carol Bailey, Technology and Business Magazine February 22, 2002
http://archive.infoworld.com/articles/hn/xml/02/09/27/020927hnmsvpnflaw.xml

11. "Windows 2000 : Virtual Private Networking" Thaddeus Fortenberry
New Riders Publishing, copyright 2001, Pgs 44-45, Pgs 145-147

12. Layer Two Tunneling Protocol "L2TP"
Network Working Group W. Townsley, et al Request For Comments : 2661
Category Standards Track, 1999
http://archive.infoworld.com/articles/hn/xml/02/09/27/020927hnmsvpnflaw.xml

13. Microsoft Security Bulletin MS02-063
Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks (Q329834) October 30, 2002
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-063.asp

© SANS Institute 2003, Author retains full rights.