Global Information Assurance Certification Paper

Security and configuration considerations of an IPSEC/VPN implementation in a NATed environment under Windows 2000, 2003 and XP

Bruce Edwards
GIAC Security Essentials Certification (GSEC)
Version 1.4b

Option 1
4 May 2004

Security and configuration considerations of an IPSEC/VPN implementation in a NATed environment under Windows 2000, 2003 and XP

Abstract

There are several considerations in providing remote access to corporate assets that workers need to utilize. In most organizations you may have people that need to perform tasks for their jobs 24/7. To accommodate these needs many companies have implemented remote access mechanisms. In the Windows environment there have been a number of challenges. The very properties that many developers and users depend on can be a significant vulnerability if exposed unprotected to the outside network. To counter these threats many companies have implemented firewalls or IP filtering solutions. Whereas this might be a good component of Defense in Depth, it does cause problems in providing access to these remote users. With many current broadband types of access, remote computers are provided with dynamic IP assignments. This can cause a significant management problem. This becomes a reactive situation and doesn't scale well since one has to continuously update the firewall as the IP address change. A more attractive solution can be to implement a VPN solution. This can provide a number of bonuses from the security prospective if designed correctly. You can now design policies and enforcement by being able to identify machines in this category and by the routes that they must use to access the corporate network. By providing this common access path you must manage the access control through this gateway rather than for each machine. This simplifies the security controls on these other machines and makes the management less complicated since the remote access routing and authentication is being handled by the VPN. This isn't to say that you should not follow up on additional security measures. You would want to provide much of these without remote access (Such as more restrictive ACLs, etc) Just because someone gains access through the VPN doesn't mean other security measures shouldn't be taken. There are issues with implementing VPNs and one must be aware that what can work inside the corporation with company owned and managed machines may not work as well as machines outside of the company ownership. By being aware of what client environments exist and the limitations they may pose, you can better defend the corporate assets that you may be charged with protecting.

Challenges with Remote Access

As the Internet has grown, along with is has the need to protect the hosts and the network that we use to communicate. It is becoming commonplace to have some safeguards in place such as virus checkers and even host based firewall products. We are now becoming aware of the need for other tools such as auto updates on these products as well as the operating system and

applications (such as office and productivity suites). Patch management of these and other products are becoming as important as the products themselves. As these actions indicate, it is simply not enough to install these products but also vitally important to manage and understand it as well.

One additional means of protecting the network when it relates to a corporate infrastructure is by use of a VPN. It is important to note that one should understand the implications of this as the use of a VPN will make your connection appear to be from the inside of the corporate network. This paper will explore some of the factors that you should bear in mind.

There are several considerations to evaluate before you decide to establish a VPN. To insure that you have made a well-informed decision, you will want to make sure that you fully explore all these factors. First there are two common types of VPNs used today. For current windows implementations you can select SSL based VPN or IPSEC based VPN solutions[1]. The capital outlay can be very inexpensive, particularly from the client side perspective for either solution. The SSL VPNs are really designed for more granular access and have very little work that needs to be done at the client side. At most you may require a small applet or utility on the client side. Most of the work and expense occurs on the server side. IPSEC solutions are intended as a more encompassing solution because they operate at a lower level on the network stack and appear to truly extend the network at this lower level. If your needs are more general in nature you may want to consider the extra complication of an IPSEC VPN. For small IPSEC VPNs the infrastructure components may already exist or may be available at very low cost. Depending on the size of the VPNs required (How may simultaneous SA - Security Associations are needed), A moderately fast server might be all that is needed for the corporate side of the VPN tunnel. If your needs require more power or higher throughput, other inexpensive option may allow you to reduce the load on the processor on both the client and the server side. Many NICs now have hardware assist features to offload much of the encryption functions. The 3COM 3C990[2] will allow offloading of 3DES encryption and decryption under both Windows 2000 and Windows XP. If this is not an attractive solution, separate network appliance products such as the Linksys BEFSX41/BEFSR41/BEFVP41[3]. The BEFSX41 is a good economical solution for a client setup that desires NAT functionality as its performance exceeds a typical DSL or cable modem bandwidth even with multiple tunnels.

---

[1][1] Phifer, Lisa. VPN:TUNNEL VISIONS How do SSL VPNs match up with their older IPSEC cousins. Information Security Magazine. August 2003 . URL: http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss21_art83,00.html . (02 Feb 2004)

[2] 3COM Corporation. EtherLink 10/100 PCI Network Interface Card with 3XP Processor User Guide. May 2000. URL: http://support.3com.com/infodeli/tools/nic/3cr990/UsrGd_11.pdf . (02 Feb 2004)

[3] Higgins, Tim. Toms' Networking, Product Review – Linksys EtherFast Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint (BEFSX41). 06 July 2002. URL: http://www.timhiggins.com/Reviews-17-ProdID-BEFSX41-1.php . (12 April 2004)

The BEFVP41 can be a good solution for requirements needing many more SAs at the expense of a lower bandwidth and a little higher price.

VPNs and NAT

As has been noted before in various papers and other sources[4], for IPSEC VPNs and NAT to work together requires several key components to be coordinated. At its basic level, IPSEC VPNs are comprised of the Authentication Header (AH), Encapsulated Security Payload (ESP) and Internet Key Exchange (IKE) Protocols.[5] Unfortunately in it's basic form there are a few things that don't work in a NATed environment. The very thing that the AH protocol depends on is altered if a VPN tunnel transverses a NAT router or firewall. Your choice here is to implement a tunnel with its end point at the Router or to allow the VPN tunnel to transverse the NAT router. To achieve this, the router must comply the NAT-Traversal (NAT-T) IETF draft[6] (The current draft at this time is draft 8 however the Microsoft implementation of L2TP/IPSEC is based on Draft 2 and RFC 3193). The other issue that can cause some difficulties is handling the IKE functions. The use of pre-shared keys is generally not as desirable because of the possibility of weak keys[7] as well as managing the keys as well. The general problems of pre-shared keys is also discussed in a FAQ on VPNs hosted by Microsoft under the question "Why are pre-shared keys non-secure?"[8] A better solution is to use a certificate based system or a Smartcard type of system.

To help determine what will be work in your situation, it is helpful to know the protocols that are being used in each of the possible scenarios. In the case of a remote host on Windows 2000/XP/2003, Microsoft has implemented sort of a hybrid configuration. The most common setup is L2TP/IPSEC. The reason for this was rooted in the state of these protocols at the time that Windows 2000 was released .The L2TP was included to provide a more convenient user authentication and endpoint assignment[9]. All that is required of the remote user

---

[4] Aydin, Haluk. Nat Traversal: Peace Agreement Between NAT and IPSEC. SANS Institute. 12 August 2001. URL: http://www.sans.org/rr/papers/index.php?id=731

[5] Schaefer, Norma Jean. Knock Knock…Who's there? Do you know who is accessing your VPN?. SAN Institute. 01 December 2001. URL: http://www.sans.org/rr/papers/index.php?id=755

[6] Kivinen, Tero. et. al. Negotiation of NAT-Traversal in the IKE. The Internet Engineering Task Force. 10 February 2004. URL: http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-08.txt

[7] Pliam, John. Authentication Vulnerabilities in IKE and Xauth with Weak Pre-Shared Secrets. 02 October 1999. URL: http://www.ima.umn.edu/~pliam/xauth/

[8] Microsoft Corporation. Virtual Private Networking: Frequently Asked Questions Number 46, 21 July 2003. URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/vpnfaq.mspx

[9] Phifer, Lisa. Windows 2000's VPN-Related Security Issues. ISP-Planet. 27 March 2000. URL: http://www.isp-planet.com/technology/vpn_windows2000a.html

is to run through the VPN wizard and then you can enable by a simple click on a shortcut. This makes the connection appear as a "Dialup Connection". With Microsoft's implementation, the user issues a password that the VPN server would generally authenticates with the domain. With this configuration it has the advantage of no additional cost at the client side, it is host based so additional computers that exist in the household are not involved with the VPN, and it will work with the existing low cost NAT and NAT/firewall appliances. This also is running on a non-split tunnel mode so that the only route is through the VPN (VPN Split tunnel modes are discussed later under Security Policies).

There are several things that one should be aware of that have a major effect on this connected computer and in fact on the corporate network as a whole. The lessons learn with general computer security apply here as well. The very thing that VPNs provide can be a significant security risk as well. The fact that the VPN provides what appears to be an internal IP address means that any trusted relationship that internal computers that are based on these internal addresses will apply to the VPN connected computers as well. This can be a flawed assumption since in many environments this remote computer may not undergo the same requirements the internal corporate computers may. The risk isn't just limited to the effects that the external connection has on the internal network though. For example, many home computer setups may include a DSL/Cable/Firewall such as the Linksys BEFSX41. Even without the Firewall functions of these routers, many may rely on the NAT function to shield the local private LAN from external probes and attacks. This practice may be somewhat effective under some conditions, but should not be considered an adequate defense because some attacks can probe the existence of a router (and computers behind them) and more significantly for this discussion the existence of a VPN link in effect bypasses the NAT function. The address of the local computer now is one that is provided by the server side of the VPN connection. This problem exists with both tunnel based VPN connections and end-point based connections. Other problems exist due to attacks that use email or the web. Being behind a NATed router will not offer you any protection with these vulnerabilities. Clearly the "Defense in Depth" advocated by SANS and others should apply here. Some of the practices that one might employ on both sides of the VPN will be discussed in more detail later on.

Security Issues with Remote Computers

First we will discuss the issues relating to the remote computer and network. Since these issues affect the security of the network these also have a direct bearing on the corporate networks security as well. In the case that the DSL/Cable router is just providing a pass though you can still utilize some aspects of the router. Routers that provide SPI (Stateful Packet Inspection) like the previously mentioned Linksys router can provide a measure of protection if they can be configured with the restrictive policies allowed. Of course one should use best practices on the general configurations on the router regardless such as using non default settings for the local IP address used for the remote

computers. If you use DHCP to grant the private addresses, use a significantly different starting address and range of the DHCP granted addresses. If the router is probed and identified then the DHCP granted address would not be the ones that an attacker may assume are granted by identifying the router. If a static address is used, don't use the default range for DHCP and don't start near the beginning of the address range if possible. Filters on the router are very valuable tools as well. Blocking ports that you will never use will be time well spent. Attention to the address range above the Well Known Ports can be straight foreword.

Use of the netstat –ao command on XP or use of Fport[10] can help identify some ports that are being used. Some web sites have documented the step you can take to minimize these services and thus allow you to block them as well[11]. Remember Defense in Depth suggests both blocking and disabling non-needed services.

Blocking outbound ports can be useful as well because many Trojans, viruses and worms use this for control and to infect other machines. This helps you to be a good neighbor and if you log (covered later) you can spot problems on this machine and help prevent problems on the corporate network. You can look at the bulletins on Blaster and Slammer to illustrate the value of filtering both directions. Slammer also demonstrates the need to inspect this as many people thought that they did not have SQL Server on their machines but did have MSDE as part of a bundled product. The use of SQL or MSDE does not preclude you from blocking this at the router but for a VPN solution you will need to provide a host solution as well.

Enabling logging on the routers and frequent inspection of these logs can give you an indication of what is going on and help trace problems. Normally these logs reside on the router but can be exported with a tool like the "Kiwi Syslog Daemon" and "Kiwi Secure Tunnel"[12] or 3Com's offering[13] for routers that use the Syslog format like Netgear. For Linksys equipment you will need an SNMP daemon. Many logging analyzers exist and are provided by the vendors and third parties. Wallwatcher[14] provides some tools for Linksys routers. Most of these are available at no extra cost.

---

[10] Foundstone. Fport – TCP/IP Process to Port Mapper.
05 June 2002. URL:
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/fport.htm

[11] Marchand, Jean-Baptiste. Minimization of network services on Windows systems.
Herve Schauer Consultants. 09 February 2002. URL:
http://www.hsc.fr/ressources/breves/min_srv_res_win.en.html
.(03 April 2004)

[12] Kiwi Enterprises. Kiwi Syslog Daemon. 28 February 2003. URL:
http://www.kiwisyslog.com/info_syslog.htm
.(13 April 2004)

[13] 3COM Corporation, A freeware Syslog service for Windows NT
http://support.3com.com/software/utilities_for_windows_32_bit.htm

[14] Wallwatcher. A Free Log Viewer for the Linksys BEF Series of Etherfast Routers.
30 March 2004. URL:
http://www.wallwatcher.com/

Either disabling SNMP or altering the SNMP setup including passwords on the router is a good idea, as SNMP will expose a lot of information that you are inquiring about. SNMP based on versions 1 and versions 2 are very insecure and can be an open window (and in some cases and open door) to your network.

If you are setting up VPN access there are a number of things that you can you can do to help the situation. You can setup a basic security policy that specifies the to minimum requirements for the remote side and then use Active Directory Policies to enforce them. The first thing you need to do is to determine what these policies are. If these policies are reasonable you should be able to get support from both the users and any company authorities that any of your security policies are approved by. This should be a reasonable requirement for access to the corporate network, and most people will find that in protecting the network, their own machine is better protected as well. Everyone's remote access security policy will be slightly different, but as a starting point, an initial policy and enforcement mechanism should be documented. If you choose to implement Group Policies to enforce a security policy you should be aware that "Modern" Windows operating systems will not apply some Group Policies by default on "slow" network links by default and in addition to setting the Group Policy you must either change the definition of "slow" links or provide an override for these policies. These settings and descriptions are documented[15], and relate to some policies like application deployment or folder redirection that you may want to use to enforce a security policy. The reason for these defaults is to avoid excessive delay or bandwidth reduction during the execution of these policies. The problem is that if you are counting on these Group Policy settings to implement your security policy, you can be deceived into believing that the remote computer is secured based on your Group Policy settings. This points out the need for verification of your security settings. Think of this in the same that you would virus scanning and virus scanning Settings (Making sure the Scanner is running and that it has up to date signature files), or patch updates. Setting and verifying key policies are always a good idea, because at any time seemingly unrelated events can prevent your carefully crafted policies from being executed (a new patch, or a Group Policy that negates or overrides yours). We will discuss some of verification solutions shortly.

There are several ways that you can enforce policies with "Modern" Windows operating systems. Using Group Polices you can configure many security related policies like Local and Account Policies. Under Windows XP and Windows 2003, Microsoft has extended this to allow you to tailor to more specific targets (i.e. all machines at a certain service pack level or the existence or non-existence or certain patches). Microsoft has also included software restriction policies in both Windows XP and Windows 2003[16]. This allows you several ways

---

[15] Microsoft Corporation. Default Behavior for Group Policy Extensions with Slow Link (KB 227369). 13 November 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;227369

[16] Microsoft Corporation. Using Software Restriction Policies to Protect Against Unauthorized Software. 01 January 2002. URL: http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx

to identify software, and blocking their execution. The implantation need not be obtrusive; your goal is to protect the machine and corporate network from attack. This is a goal that all concerned can appreciate.

The Importance of Security Policies

Developing a good security policy is perhaps one of the most overlooked aspects of protecting the computing environment. Although organizations such as SANS and others do stress the need and importance of developing a good security policy, many people tend to consider it mundane and uninteresting. In reality, by designing a good security policy you are creating a good blueprint for all the rest of the work that you need to do to secure the corporate network.

There are specific challenges to designing a security policy that will work in many VPN environments. Some of the issues revolve around what you can realistically do as many machines and part of the infrastructure are privately owned or separately maintained. If you are too heavy handed in developing this security policy by making it too difficult to implement, too restrictive or too difficult to change you may find that people may try to circumvent these policies. This is like the homeowner building an addition without going through the permitting process. The design and implementation of your security policy shouldn't difficult or onerous. The security policy should be a living document with the understanding that it will change as needs and conditions evolve. By educating people about the larger picture and providing solutions that both protect and allow these remote users to accomplish their work, everyone benefits. It is in everyone's best interest to work in a secure computing environment. The CERT[17] discusses some guidelines and provides education for computer security at home that would be good to have people adapt even if you do not include this in your company security policy. Another good paper on security policies as it relates to remote VPN issues is Todd Rosenberry's GSEC Practical paper "Protecting Your Corporate Network from Your Employee's Home Systems"[18]. In this paper from the SANS Reading Room he discusses some of the ways that security can be compromised and the steps to mitigate these risks. In particular he does reference a paper written by Stuart Broderick titled "Implementing and Managing a VPN Security Policy"[19]. Here Stuart outlines several pertinent VPN policies and then explains why these policies are important. You will generally get agreement from most people that security is important, but many people don't realize how vulnerable they are or believe that it won't happen to them. Todd does discuss some trade offs that you might want to think about. Some points

---

.(23 April 2003)
[17] CERT Coordination Center. "Home Network Security ", 22 Jun 2001. URL: http://www.cert.org/tech_tips/home_networks.html
.(05 December 2001)
[18] Rosenberry, Todd. Protecting Your Corporate Network from Your Employee's Home System. SANS Institute. 21 December 2003. URL: http://www.sans.org/rr/papers/50/1314.pdf
[19] Broderick,Stuart,PhD. Implementing and Managing a VPN Security Policy . Symantec. 23 Apr 2002. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=1298&EID=0

need to be re-evaluated in light of the changing security landscape on the Internet. For example, since higher speed broadband is more commonplace and higher speed PCs are available at less cost, some choices might want to be made in favor of better, more easily configured, and better enforced security. The choice of "Split Tunnels" for VPN trades off bandwidth and processor overhead for allowing alternate routes into the remote computer should be discouraged. Todd does warn of the dangers of this but indicates that precautions can be taken to alleviate this. As the complexity of managing the network and computing environment increases, the greater the risk is of introducing an inadvertent pathway that an exploit can employ. Defense in Depth stresses applying security wherever you reasonably can. By simplifying the management of the implementation and enforcement of these policies you lessen the chance of error and you reduce the possible exposure to vulnerabilities. You will be always dealing with undiscovered exploits and by restricting those mechanisms that you can you will be better off. So if it means restricting services or ports or routes that you don't need, then everyone is better off (except for those who want to exploit the computer or network). Including a good password policy is very important. You desire something that is relatively secure but not something that is to difficult to deal with so that the user will circumvent the policy by sticky notes on the monitor or worse yet stuck in a file somewhere. One possible approach is to use a utility such a Keypass[20]. This is a utility that manages a username/password database that encodes it using AES. Just one password is needed to open it and any cutting and pasting of username and passwords are only on the clipboard of 10 seconds. You don't even see the password in this operation. This allows the use of complex passwords without undue burden on the end user. This also can encourage the use of different passwords for different accounts because the user doesn't need to remember all of the passwords.

Implementing your Security Policies

The difficult process is determining what the security policies should be. If you accept computers not owned or operated by the company but allow them access to the network, it can be a bit of a balancing act. When you are trying to design a policy that will both protect the corporate network but be acceptable to the owners of the external computers you may need to make some compromises. If you structure policies that implement these common goals you may find them more likely to be accepted. Several sources have come up with suggested lock down procedures such as Microsoft[21] and others[22] You may find

---

[20] Reichl, Dominik. Keypass Password Safe. Sourceforge. 07 March 2004. URL: http://keepass.sourceforge.net/
(24 March 2004)

[21] Microsoft Corporation. Windows XP Security Guide. 22 May 2003. URL: http://www.microsoft.com/downloads/details.aspx?FamilyId=2D3E25BC-F434-4CC6-A5A7-09A8A229F118&displaylang=en
.(28 January 2004)

that the extent of the suggestions may prevent operations of processes or programs needed or desired. In formulating this policy you must determine what risks exist to determine what policies to implement. Remember, these are suggestions and you must determine what will work best in you environment.

You can use several tools to help verify settings and determine where they are being set. Gpresult[23] is a command line tool that is useful as both a diagnostic and a verification tool. WMI has the ability to retrieve and set all sorts of information. You can retrieve registry information that could tell you the version or the creation date of your virus signature file. You aren't going to be able to check everything but checking key settings or unusual behavior will alert you to a potentially harmful situation. These suggestions also are useful for non-VPN machine but in many VPN environments you may not have as much control of the machine initially. There are several aspects of your policies that you may want to be able to verify to insure that the security policy is being properly executed.

Security Policy Enforcement

After your verification process you are now in a better position to enforce these polices. As we have touched on before, there are several mechanisms that you can use to insure that these polices are followed. By logging into a domain, you can use "Software Restriction Policies" to determine what you need to do. If the machine that is attempting to log into the Domain fails any of these policies, you can move it to an Organizational Unit or a group of Organizational Units that have severely restricted access. The purpose of any machines that you would have access to would be to provide you with the means to rectify the security policy violation. For example, if you are logging in and a Critical Hotfix has been released that you have deemed necessary for the base security policy, the remote machine would be moved into one of these restrictive OUs. You now can now according to the security policies that you have prepared any number of mechanisms to correct the violation. You could require Automatic Update service to be running and send a message to the remote machine that it needs to update the computer. You can send a message for the owner to run Windows Update (and provide access). You could provide copies of the Hotfixes that the owner could run or provide a local repository for products like HfnetchkPro Lite[24]. Providing a local store for these patches or Hotfixes serve several functions. You are able to isolate a vulnerable or compromised machine and you are able to provide a local cache that is available in case the Vendors

---

[22] Jansson, Markus. , How to secure Windows2000 / XP. 2003. URL: http://www.markusjansson.net/exp.html

[23] Microsoft Corporation. How to Use the Group Policy Results (GPResult.exe) Command Line Tool. 25 October 2001. URL: http://www.microsoft.com/windowsxp/pro/using/itpro/managing/gpresults.asp

[24] Shavlik Corporation. HFNetChkPro and HFNetChkPro Lite. 07 April 2004. URL: http://www.shavlik.com/

site is overloaded or unavailable. You need to balance how you enforce compliance with the security policy because for a lot of machines that may be accessing the corporate network may not be owned by the corporation. Using techniques that deploy these patches such as SUS[25] or Shavlik's HFNetchkPro may preclude the owner's involvement and may be difficult to include in the company's remote security policy. By restricting access to only those resources needed to correct the problem you have provided a way of protecting the corporate network, protecting the remote host and allowing the problem to be resolved without intervention of the Help Desk. Not having to staff the Help Desk 24/7 or have an IS person responding to calls after hours because someone can't access the network for a project or presentation that is due the next morning reduces the stress level for everyone. As part of the security policy you also need to educate the remote users what to expect when some violation occurs to the security policy so that if and when it occurs the steps requested won't be a surprise to them. You don't need to discuss in detail what needs to be done (although some people may want to know the details), because you can include this in the message to be sent out when the violation occurs. Obviously you need to enforce other portions of the policy as well. Checking to make sure a virus scanner is installed, running and enabled with up to date virus files should be part of the policy. This should be something that once the remote host is setup violations should not occur unless something fails as much of the updates can be automated as well. Keeping a local repository of the updates and signature files should be part of the policy for the same reasons you would keep a local cache for patches and Hotfixes. Information about the existence, versions and status of virus checking software can be access through WMI[26] and/or the Remote Registry Service. These infrastructure pieces are part of the checks that you need to employ and indicate any failures to the remote user so that a fix can occur (Like start and set to automatic the Remote Registry Service for example). Security policy enforcement of a remote firewall service is a little more dependent on what firewall policy you have. Much of how you develop your policy with respect of firewalls is somewhat dependent on choices that you will need to determine. At the very least you should mandate a host base firewall that deals with both ingress and egress traffic. The ingress aspect is generally obvious as you are restricting access to the remote host from possible exploits. The egress aspect of the firewall protects the corporate network from a possible compromised machine. If the remote user sees attempted access to a site, the user will be alerted to the attempted access. Products such as Zone Alarm[27] provide an inexpensive and effective protection. You may want to consider a few

---

[25] Microsoft Corporation, SUS with SP1 Release Notes and Installation Instructions. 04 February 2003. URL:
http://www.microsoft.com/windowsserversystem/sus/sp1relnotes.mspx
(07 April 2004)

[26] Microsoft Corporation. Windows Management Instrumentation.
April 2004. URL:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/wmi_start_page.asp

[27] Zonelabs. Zone Alarm. April 2004, URL:
http://www.zonelabs.com/store/content/home.jsp

settings in increase the robustness of these key programs. As some exploits will try to disable key services and programs you can employ a couple of techniques to make it more difficult and to insure that the security policy is being followed. For patches you may want to have the remote user run the Automatic Update Service[28] to make sure that patches get updated as soon as possible. With product such a Zone Alarm you can require the use of a password to alter any security settings. Where exploits can currently alter settings it is much more difficult to have the exploit respond to a password prompt. Although it is not feasible to expect all remote users to install an Intrusion Detection System, Using a program like RegRun[29] or StartupMonitor[30] will alert the user to attempt to register itself at startup. If you get popups from either of these programs indicating startup changes when it isn't expected, you may want to investigate.

Educating the users on the operation of these tools is a very important aspect of maintaining the security. They need to be brief on the expected an unexpected operations. They need to know how they can safely respond to and what to expect. If they see the Truevector engine shutting down and they are not doing it themselves or updating Zonealarm, this should raise a red flag. If the Virus Checker is disabled this should be investigated. If they can't run Windows Update or Auto Update fails they should communicate this. It is far easier to deal with problems at this level then to need to deal with a security breach later.

Conclusion

In conclusion, to achieve a well managed, secure VPN solution you should go through the security policy design and make sure that the choices you make are supportable, manageable and secure. There will always be trade offs, but everyone's goal should be one of security. As each organization is different, your policy will be different. You need to be conscious that these solutions aren't really plug and play, but they need to be carefully developed. You should be aware of the challenges that exist with VPN environments and dealing with computers that you may have little authority on. A good security policy that all subscribe to is one of the best ways of being able to put in the necessary safeguards.

---

[28] Microsoft Corporation. HOW TO: Configure and Use Automatic Updates in Windows 2000 (KB 327850). June 2002. URL: http://support.microsoft.com/default.aspx?scid=327850 (29 April 2004)

[29] Greatis Software. Run Reg II Security Suite. 26 April 2004. URL: http://greatis.com/regrun3.htm

[30] Lin, Mike. StartupMonitor. 20 May 2000. URL: http://www.mlin.net/StartupMonitor.shtml

References

[1]Phifer, Lisa. VPN:TUNNEL VISIONS How do SSL VPNs match up with their older IPSEC cousins. Information Security Magazine. August 2003 . URL: http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss21_art83,00.html

[2] 3COM Corporation. EtherLink 10/100 PCI Network Interface Card with 3XP Processor User Guide. May 2000. URL: http://support.3com.com/infodeli/tools/nic/3cr990/UsrGd_11.pdf

[3] Higgins, Tim. Toms' Networking, Product Review – Linksys EtherFast Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint (BEFSX41). 06 July 2002. URL: http://www.timhiggins.com/Reviews-17-ProdID-BEFSX41-1.php . (12 April 2004)

[4] Aydin, Haluk. Nat Traversal: Peace Agreement Between NAT and IPSEC. SANS Institute. 12 August 2001. URL: http://www.sans.org/rr/papers/index.php?id=731

[5] Schaefer, Norma Jean. Knock Knock…Who's there? Do you know who is accessing your VPN?. SAN Institute. 01 December 2001. URL: http://www.sans.org/rr/papers/index.php?id=755

[6] Kivinen, Tero. et. al. Negotiation of NAT-Traversal in the IKE. The Internet Engineering Task Force. 10 February 2004. URL: http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-08.txt

[7] Pliam, John. Authentication Vulnerabilities in IKE and Xauth with Weak Pre-Shared Secrets. 02 October 1999. URL: http://www.ima.umn.edu/~pliam/xauth/

[8] Microsoft Corporation. Virtual Private Networking: Frequently Asked Questions Number 46, 21 July 2003. URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/vpnfaq.mspx

[9] Phifer, Lisa. Windows 2000's VPN-Related Security Issues. ISP-Planet. 27 March 2000. URL: http://www.isp-planet.com/technology/vpn_windows2000a.html

[10] Foundstone. Fport – TCP/IP Process to Port Mapper. 05 June 2002. URL: http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/fport.htm

[11] Marchand, Jean-Baptiste. Minimization of network services on Windows systems. Herve Schauer Consultants. 09 February 2002. URL: http://www.hsc.fr/ressources/breves/min_srv_res_win.en.html .(03 April 2004)

[12] Kiwi Enterprises. Kiwi Syslog Daemon. 28 February 2003. URL: http://www.kiwisyslog.com/info_syslog.htm .(13 April 2004)

[13] 3COM Corporation. A freeware Syslog service for Windows NT. 21 September 2000. URL: http://support.3com.com/software/utilities_for_windows_32_bit.htm

[14] Wallwatcher. A Free Log Viewer for the Linksys BEF Series of Etherfast Routers. 30 March 2004. URL: http://www.wallwatcher.com/

[15] Microsoft Corporation. Default Behavior for Group Policy Extensions with Slow Link (KB 227369). 13 November 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;227369

[16] Microsoft Corporation. Using Software Restriction Policies to Protect Against Unauthorized Software. 01 January 2002. URL: http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx .(23 April 2003)

[17] CERT Coordination Center. "Home Network Security ", 22 Jun 2001. URL: http://www.cert.org/tech_tips/home_networks.html .(05 December 2001)

[18] Rosenberry, Todd. Protecting Your Corporate Network from Your Employee's Home System. SANS Institute. 21 December 2003. URL: http://www.sans.org/rr/papers/50/1314.pdf

[19] Broderick,Stuart,PhD. Implementing and Managing a VPN Security Policy . Symantec. 23 Apr 2002. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=1298&EID=0

[20] Reichl, Dominik. Keypass Password Safe. Sourceforge. 07 March 2004. URL: http://keepass.sourceforge.net/ (24 March 2004)

[21] Microsoft Corporation. Windows XP Security Guide. 22 May 2003. URL: http://www.microsoft.com/downloads/details.aspx?FamilyId=2D3E25BC-F434-4CC6-A5A7-09A8A229F118&displaylang=en .(28 January 2004)

[22] Jansson, Markus. How to secure Windows2000 / XP. 2003. URL: http://www.markusjansson.net/exp.html

[23] Microsoft Corporation. How to Use the Group Policy Results (GPResult.exe) Command Line Tool. 25 October 2001. URL: http://www.microsoft.com/windowsxp/pro/using/itpro/managing/gpresults.asp

[24] Shavlik Corporation. HFNetChkPro and HFNetChkPro Lite. 07 April 2004. URL: http://www.shavlik.com/

[25] Microsoft Corporation, SUS with SP1 Release Notes and Installation Instructions. 04 February 2003. URL: http://www.microsoft.com/windowsserversystem/sus/sp1relnotes.mspx (07 April 2004)

[26] Microsoft Corporation. Windows Management Instrumentation. April 2004. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/wmi_start_page.asp

[27] Zonelabs. Zone Alarm. April 2004, URL: http://www.zonelabs.com/store/content/home.jsp

[28] Microsoft Corporation. HOW TO: Configure and Use Automatic Updates in Windows 2000 (KB 327850). June 2002. URL: http://support.microsoft.com/default.aspx?scid=327850 (29 April 2004)

[29] Greatis Software. Run Reg II Security Suite. 26 April 2004. URL: http://greatis.com/regrun3.htm

[30] Lin, Mike. StartupMonitor. 20 May 2000. URL: http://www.mlin.net/StartupMonitor.shtml

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event