Global Information Assurance Certification Paper

The 'inside-out' threat: The VPN solution's weakest link; the VPN user.

Eric R Rosander

February 13, 2001

Introduction

This paper is intended as a discussion on security concerns after the Virtual Private Network (VPN) connection has been made, the potential threats, and some of the things that can be done to minimize these threats. The document focuses mainly on the home VPN user and the threat of 'always on' internet connections, but some of the concepts apply to remote and branch office VPNs as well. It assumes a basic understanding of VPNs, and common Industry terms and acronyms. See Virtual Private Network (VPN) Security **by** Gregory J. Ciolek, January 4, 2001 for more information on VPNs.

A real world example:

Not too long ago, a client of mine contracted me to assist in creating a VPN connection between one of their servers and a database consultant's home network. This DBA consultant required remote access as he lives a considerable distance away. We were linking the VPN between his SOHO class cable modem firewall and my client's larger enterprise class firewall. My employer and the DBA had already worked out the details; both firewalls were IPSEC compliant, they had pre-determined that they were going to use 3DES and MD5 with a shared secret to create the VPN. The DBA would then have full database administrative rights to the development and production databases, a full read/write share on their server, and therefore, has an account on their Windows NT domain. The client felt comfortable with this, thought it was perfectly secure (after all, this is a *VPN*) and all they wanted me to do was make it work.

Once I get there I phoned up the DBA consultant to start the inevitable trouble-shooting required when setting up two different vendor's interpretation of the IPSEC standard (this is a two hour job at most, right?). He turns out to be a wealth of information on his own firewall; after all, he does this all the time. He has *multiple* accounts where a similar connection to the one I was creating was set up. He also described his home Windows NT network, his new wireless setup, and how he can now work from anywhere in his house, including his back yard. Sounds like one cool setup. This is what the future should be, working at home and sitting by the pool, with broadband access and no wires.

That's scary.

This guy has full administrative rights to multiple databases in multiple enterprises. He has logon accounts to multiple networks. His 'always on' Internet access is protected by a SOHO class firewall that's well documented and possibly exploitable. Never mind the firewall, with a wireless laptop all one would need to do is sit across the street and jack in to his wireless network. A few NT exploits, wireless network sniffs, password cracks, etc., and you have a cracker's playground. I would be willing to bet that even the shared secrets for his various VPN connections is sitting on a database somewhere on his own network (and if not, it still makes a good example).

VPN Hijacking and Other Concerns

Why try to hack an enterprise with enterprise dollars and get through their enterprise level firewall and Intrusion Detection Systems (IDS), logs, etc., when you could take advantage of the above situation and hijack a trusted VPN? What if any one of the foreign trusted network's systems were simply infected by a virus, worm, or Trojan? Multiple databases could be wiped out and networks compromised from this single point.

The above scenario is very common and is just one example of a type of VPN and its potential use, in

this case hardware-based VPN access for a vendor. Typically, they may only have access to one machine or service on the network. The access is hopefully limited within the scope of their product or services.

Another example is the client-based VPN software that can be loaded on a home PC, or a laptop for the traveling user. For the majority of this kind of VPN configuration, these are fully trusted users. Their access is supposed to be the same as if they were sitting right there at work, physically inside the network. For all intents and purposes they *are* inside the network. Hopefully, steps have been taken to be sure the authenticated user is who they say they are. The use of certificates and/or software or hardware tokens can make these very secure connections.

But what happens once the connection is made? This home PC is connected to the Internet. In ever increasing numbers, they are connected with 'always on', xDSL, cable, or other broadband connection. The traveling laptop could be connected to the Internet, a hotel network, Wireless LAN, or any other unknown foreign network. What if the VPN client's machine was in one way or another compromised, either before or during that ultra-secure authenticated connection? What is keeping that home or foreign network safe from a virus? How many other household members, guests, etc., have access to that same machine? Could a Trojan on that home PC or laptop be emailing the certificate and password to a potentially hostile threat?

Many of these concerns are revisiting old problems. Remote Access Services (RAS) for users, vendors, and remote branch offices has been around for a long time. Not only do you trust the vendors, and users, etc., into your network, but potentially anyone else that has an access to that vendor's or user's network. Viruses spread by these entrusted sources have always been a threat.

In my opinion, there are two major factors that have dramatically increased the level of these threats. The first being advances in networking and Internet access. The older RAS solution revolved around dial-up connections. Dial back, hardware tokens, and other measures could be taken to make them more secure. This was often a closed, proprietary, connection. In many cases, a network connection was not necessary and the device accessed was a stand-alone, un-networked device. Now, the very idea behind a VPN is that you are utilizing the Internet, a very public and insecure network. Internet usage and high speed access is commonplace and even expected. The threats increasing even more with the introduction of Wireless Networks, of which the security concerns are outside the scope of this paper. Refer to, **Wireless LANs - the Big New Security Risk** Gordon L. Mitchell, PhD, CISSP May 5, 2000 for more on that subject.

The other major factor comes down to psychology and education. The budget dollars have been spent. Consultants have been hired, research and studies done, the best perimeter defense has been implemented, and the VPN solution that's the best fit for your organization has been rolled out. This has to be secure. It's a *VPN.* Users and upper management alike have been sold on the idea that this is a secure way of accessing their network using the Internet from the comfort of their own homes. There is a certain level of complacency and no one wants to hear that this wonderful new access is less than perfect.

What has been done so far?

Recent exploits and press worthy hacks have brought an increasing awareness to the general public regarding 'always on' Internet connections. The industry has responded in kind with a large selection of SOHO firewall appliances and/or personal firewall software that can be loaded on the Internet connected device to protect them from common Internet threats. (See Protecting your Home Computer from the Internet, Can You Keep the Heat Out? Robert Ashworth December 9, 2000) Many of these solutions are free, or with some luck, offered as part of the service from the Internet Service Provider (ISP). Projects like the RCF Linux firewall or the Linux Free S/WAN "build it yourself" SOHO firewalls also help to increase user awareness and provide easier tools to configure a safe Internet connection or gateway.

Newer SOHO routers/firewall devices can be configured to disallow all other traffic while a VPN is established, also enforcing that the connection be temporary. Some are even client-based VPN software "aware", with rules that allow IPSEC traffic through their NATed or Masqueraded connections. The Linux projects mentioned above can also be configured to allow IPSEC traffic through. There are also a few Windows based firewall/gateways that can be configured to work with IPSEC traffic. At minimum, these firewall, gateway, and personal firewall client solutions should be protecting the Internet connected device, as well as a good virus-scanning package.

Unfortunately, many of these SOHO firewall devices do not work well with IPSEC traffic and most, if not all, of the personal firewalls are not compatible with the client-based VPN software solutions. The Linux and Windows home gateways work great, and you can configure them precisely to your specifications, but they are way beyond the standard user's technical capabilities. Most of the time, in order to establish the VPN, the client needs to be outside the firewall or the personal firewall software needs to be disabled, leaving them, once again, vulnerable.

Two of the major client-based VPN vendors that I have worked with deal with this problem directly. Check Point's SecuRemote client now also comes with an optional SecureClient product that an administrator can configure by using "policies". The product works like a personal firewall, and monitors the client's network traffic to limit the chances of the VPN traffic being hijacked. You can create a policy limiting the type of interface or network protocol that is configured on the client. As an example, a Wireless NIC could not be added without the administrator's intervention.

Cisco's VPN Concentrator Client (once Altiga), by default, also limits VPN hijacking. Once the VPN connection is established, the client is issued an IP address and gateway from your internal network's pool of addresses limiting any other traffic to that device. Internet traffic is actually re-directed out your default routes like any other device on your network. This has the added benefit of enforcing internal network policies, like web filtering, while the device is on the VPN.

What more can be done?

No solution is perfect. The risk will always be there as long as Remote Access of any sort is allowed into your network, including VPNs. Steps can be taken to ensure that the risk is kept to a minimum.

- **Know your network**

  Nothing can take the place of the educated and aware administrator. Before your VPN is deployed, make sure you know what is on your network. Just because the client is to appear as if it was on the network, does not mean that they necessarily need access to every thing on the internal network. Are you an insurance company with a connection to the DMV? Can your billing department run credit checks? Steps can be taken to ensure that gateways to restricted or sensitive information never becomes a part of your encryption domains. Design carefully. Log everything you can and review the logs often. Get to know trends and investigate "suspicious" behavior.

- **User Education and Policy**

  User education and Policy can never be stressed enough. Most of the time, the VPN user's PC is their personal property and beyond your control. The user should be educated in Internet safety practices, ensure that virus scanning software and some sort of firewall, either hardware or software, is protecting that Internet connected device. A part of your overall VPN policy should include some sort of user sign off, outlining who is responsible for support and maintenance, such as virus signature updates. The policy should also outline appropriate usage. Access from home should be taken as seriously as access at work. Just because you work for the DMV and can now log in at any time doesn't mean you can run license plate checks on your neighbors, nor should another member of the household or guest have that access. Getting a signed policy into place can save you your job.

Get at least a rudimentary policy in place from the start, before you allow the first VPN connection. Based on experience, “pilot” projects can get out of hand and become “production” before you know it. Granting VPN access is like handing out candy, many will want it that never had an apparent “need” before. (“See honey, now I *need* that new PC with DSL access, so I can work from home”).

- **Restrict what you can**

As in the case of the opening example, ensure that the vendor or user is restricted to only the absolute servers or services needed. If possible, restrict access to your network to only come from a single device on the other network. Try and enforce time restrictions, ensuring that the ‘always on’ connection is not ‘always connected’.

Closing Summary

The deployment of VPNs is on the rise. Chances are that if you are involved in network security you already have or will be involved in a VPN project. An abstract from IDC’s **IP VPN Services: U.S. Market Forecast and Analysis, 2000-2005** states “The IP virtual private network (VPN) services market for U.S.-based carriers will grow rapidly, from $1.28 billion in 2000 to almost $10 billion in 2005.” This rate of growth makes VPNs one of the fastest growing segments of the IT industry.

You can increase enterprise security by deploying and, where possible, centrally managing firewalls for all your remote clients. Steps need to be taken to prevent the "hijacking" of established VPN connections for remote clients using unsecured broadband Internet access services such as cable modem or DSL. It also helps to ensure that the users’ desktops are configured securely before they are granted VPN access. As with any security project, you are only as secure as your weakest link.

Sources:

Joel Scambray, Stuart McClure, George Kurtz:
Hacking Exposed: Network Security Secrets and Solutions

PracticallyNetworked VPN help page:
http://www.practicallynetworked.com/support/VPN_help.htm

SecurityWatch.com
VPN Products list: http://www.securitywatch.com/scripts/links/list.asp?CID=5
Business News: Cisco Systems and Network Associates VPN Client interoperability
http://www.securitywatch.com/newsforward/default.asp?AID=434
http://www.nai.com/products/security/vpnclient.asp

Tina Bird: Virtual Private Networks: Foundation and Practical HOW-TOs
SANS2000 Course Book, March 23,2000

PhoneBoy’s Firewall-1 FAQ page
http://www.phoneboy.com/fw1/

The Linux VPN Masquerade HOW-TO
http://www.impsec.org/linux/masquerade/ip_masq_vpn.html

PBS Frontline: Hackers, aired February 16, 2001
http://www.pbs.org/wgbh/pages/frontline/shows/hackers/

CNET News.com February 6, 2001 Commentary: Group discovers wireless security hole
http://news.cnet.com/news/0-1004-201-4730941-0.html?tag=prntfr

InternetWeek Online: Enterprise Communications Start Migration To VPNs, September 13, 1999 http://www.internetwk.com/VPN/VPNsupp091399-1.htm

Steven T. Harris, Courtney Munroe: IP VPN Services: U.S. Market Forecast and Analysis, 2000-2005 *Report #W23565 - December 2000* International Data Corporation (IDC) Abstract http://www.itresearch.com/alfatst4.nsf/unitabsx/W23565?openDocument&q=VPN+++++

Vendors and Products

Checkpoint FireWall-1 and VPN-1 http://www.checkpoint.com/

Cisco VPN Concentrator 3000 series http://www.cisco.com/univercd/cc/td/doc/pcat/3000.htm - xtocid31410

SonicWall http://www.sonicwall.com/

WatchGuard http://www.watchguard.com/

ZDNet: Zone Labs ZoneAlarm Pro Full Review http://www.zdnet.com/pcmag/stories/pipreviews/0,9836,371562,00.html

Network Associates (NAI) PGP Corporate Desktop PGP Security - Products - PGP Corporate Desktop 7.03

SANS Level-1 Graduate Papers Referred to, and their sources:

Virtual Private Network (VPN) Security **by** Gregory J. Ciolek, January 4, 2001

Protecting your Home Computer from the Internet, Can You Keep the Heat Out? Robert Ashworth December 9, 2000

Wireless LANs - the Big New Security Risk Gordon L. Mitchell, PhD, CISSP May 5, 2000

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 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 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 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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
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
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
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