Net Admin Weekly
53,000 Subscribers Worldwide
November 27, 2002
Issue #18

Feature

Q & A

Security Advisories

News Headlines & Resources

Download of the Week

Feature

The Microsoft L2TP/IPSec VPN Client

to top

Every so often something really cool and exciting happens in the Microsoft world that you expect every Microsoft-related publication to scream the virtues of! In fact, something cool happened several months ago, but I bet you haven't heard of it, or if you did, you just saw a link to the feature and that was it. What is this "must have" thing? The Microsoft L2TP/IPSec client.

What's the big deal about the Microsoft L2TP/IPSec client? This new VPN client solves a problem that's lurked in the background since Windows 2000 was released. The one thing that kept many Windows 2000 administrators from implementing a L2TP/IPSec VPN solution was the lack of support for L2TP/IPSec for their downlevel clients. As much as we dream of new networks with nothing but Windows 2000 Pro and Windows XP workstations, it ain't going to happen. There are just too many Win9x and Windows NT 4.0 Workstation computers out there that need VPN access.

Problem solved! The new Microsoft L2TP/IPSec client now allows Win98, Win98SE, WinME, and Windows NT 4.0 Workstation computers to use L2TP/IPSec to connect to Windows 2000 and other VPN servers. Before the release of the Microsoft L2TP/IPSec client, only Windows 2000 and Windows XP computers could be L2TP/IPSec VPN clients. Now the last stumbling block to fully implementing a L2TP/IPSec VPN it out of the way.

Well, almost out of the way. The Microsoft L2TP/IPSec client does not support Windows 95. That's to be expected, since Microsoft doesn't really support it any longer either.

Software requirements for the Microsoft L2TP/IPSec client are very reasonable:

- Win98/SE – IE 5.01+ and DUN 1.4
- WinME – VPN component installed and IE 5.5+
- Windows NT 4.0 PPTP install, SP6 and IE 5.01+

Notice that you need to upgrade to DUN 1.4 for your Win98 clients. A lot of 9x admins have upgraded to DUN 1.3 and thought that was the end of it. Not true. If want to take full advantage of your Win98 VPN clients, you must upgrade to DUN 1.4.

Advantages of L2TP/IPSec over PPTP

Maybe you already have a VPN server in place and all your clients use PPTP to connect to the VPN server. Everything is working fine for you, so you don't see any compelling reason to change over to L2TP/IPSec. While PPTP is a fine VPN protocol, it doesn't match L2TP/IPSec's security and stability. Some advantages L2TP/IPSec has over PPTP include:

- Origin authentication
- Data Integrity
- Two levels of authentication – Cert/preshared key and PPP Auth

- Confidentiality

L2TP/IPSec uses IPSec in transport mode within the tunnel and allows all communications between the L2TP/IPSec client and server to authenticate their origins. This provides strong protection against man in the middle attacks.

IPSec also protects against man in the middle attacks by providing for data integrity. If any of the information moving through the tunnel is changed while in transit, the packets will be dropped by the receiving L2TP/IPSec VPN server. Confidentiality is assured by the DES or DES3 encryption protocols that can be used to hide data moving through the tunnel. While Windows 2000 and Windows XP VPN clients can negotiate DES3 encryption, Microsoft L2TP/IPSec clients can only use DES.

Probably the most obvious difference between PPTP and L2TP/IPSec connections is that PPTP only required user authentication while L2TP/IPSec requires both computer and user authentication. PPTP uses familiar PPP authentication protocols like MS-CHAP, MS-CHAPv2, and EAP/TLS. While hashing mechanisms are used to protect credentials during PPP authentication, the credentials are not protected by the VPN tunnel until after the PPTP tunnel is established. A dedicated intruder might be able to take advantage of this weakness and run a replay attack to compromise the connection.

On the other hand, L2TP/IPSec first establishes the encrypted tunnel by negotiating the IPSec security associations. The VPN client machine must have a pre-shared key or a certificate to present to the VPN server in order to establish the secure tunnel. Only after the tunnel is established does the PPP user authentication process start. Because the tunnel secures the link before PPP user authentication, the user can use any type of PPP authentication method, even clear text, and the credentials are protected by IPSec.

NAT Traversal for L2TP/IPSec

Last week I went over some of the barriers to using IPSec across a NAT device, and how the IETF plans to fix the problem (NAT-T). The Microsoft L2TP/IPSec client uses this standards-based mechanism to allow L2TP/IPSec clients behind a NAT device to connect to L2TP/IPSec servers on the Internet. This is a tremendous boon to users who need to connect to their corporate networks through a NAT device or firewall.

If you wanted to connect to a L2TP/IPSec VPN server through the NAT, you had to use a third-party solution, such as the Cisco or Nortel client. The problem with these third-party solutions is that they implement proprietary schemes that aren't standards based. A firewall administrator can easily be driven mad by trying to support all the proprietary protocols.

If you're running an all-Windows shop right now, there is a catch. The Windows 2000 RRAS does not support NAT-T. Only the Win2003 RRAS supports NAT-T, so if you want to use a Windows VPN server to support L2TP/IPSec through NAT for your VPN clients, you'll have to wait for the

release of Win2003 next April. If you already have another L2TP/IPSec VPN server in place, then you're in luck! You can start using the Microsoft L2TP/IPSec client right away to allow your VPN clients to connect through the NAT.

Another thing worth mentioning is that the Microsoft L2TP/IPSec client cannot be used to make a Windows NT 4.0 RRAS machine an L2TP/IPSec gateway. If you need to create an L2TP/IPSec gateway-to-gateway connection between Windows RRAS or third-party VPN servers, then you'll need to use Windows 2000 or Win2003.

Certificate and Pre-shared Key Authentication

The Microsoft L2TP/IPSec client needs to use either a pre-shared key or a certificate to create the IPSec connection with the VPN server. The best solution is a certificate. Certificates cannot be "brute forced" and certificate authentication is very difficult to crack. The only viable way to compromise certificate authentication is to steal the certificate.

However, if you're not prepared to put together a certificate server and public key infrastructure, you can still use the Microsoft L2TP/IPSec client to connect to the L2TP/IPSec VPN server. The alternative is to use a pre-shared key. Pre-shared keys are easy, because all you need to do is come up with a string of numbers, letters and characters (from 8 to 255 characters total) and configure the L2TP/IPSec VPN server and Microsoft L2TP/IPSec client to use the same key for authentication. However, there are some disadvantages to using a pre-shared key:

- A single key is used by all VPN clients and the VPN server
- The pre-shared key is susceptible to brute force and dictionary attacks
- There is no mechanism for "revoking" a pre-shared key in the event of compromise
- Pre-shared keys don't lend themselves to centralized management

If at all possible, you should implement at least a single certificate server and issue certificates for the Microsoft L2TP/IPSec clients from that server. One interesting and important difference between the Microsoft L2TP/IPSec client and the Windows 2000/XP VPN client is that the Microsoft L2TP/IPSec client uses *user certificates* for machine authentication. The Windows 2000/XP VPN client uses *machine certificates* for machine authentication. This is important because you need to assign user certificates to the users who use the Microsoft L2TP/IPSec client.

Remember that the VPN server will also need a certificate. You can use the Windows 2000 or Win2003 certificate server and use autoenrollment, MMC, or Web-based enrollment to assign a machine certificate to the VPN server. If you are using a third-party L2TP/IPSec server, you can have the device request a certificate from a Windows 2000 certificate server, or you can use a third-party certificate. Just make sure that the clients and server trust each other's certificate chains!

Configuring the Client

Configuring the client is easy. First, download the Microsoft L2TP/IPSec client **here** and run the installation package. Then perform the following steps:

- Click Start, point to Programs and then point to Microsoft IPSec VPN. Click Microsoft IPSec VPN Configuration.
- From the Microsoft IPSec VPN Configuration Utility dialog box, select the appropriate options for your L2TP/IPSec deployment.
- Click OK.

You can see a screen shot of the client **here**.

The pre-shared key text box supports copy and paste. This is a boon to users because typing a complex key will lead to a lot of data entry errors.

If you're working with Win2003, you should consider using the Windows 2000 Connection Manager Administration Kit (CMAK). The Win2003 CMAK is aware of the Microsoft L2TP/IPSec client. Unfortunately, you won't be able to use the Windows 2000 CMAK to create VPN connectoids for the Microsoft L2TP/IPSec client.

Summary

The Microsoft L2TP/IPSec client allows your downlevel clients to access L2TP/IPSec VPN servers. The is a major advance in Windows VPN client technology, as only Windows 2000 and Windows XP supported L2TP/IPSec VPN client connections before the release of the new client. It's even better news for those of you who need to support L2TP/IPSec through NAT devices. Give the Microsoft L2TP/IPSec VPN client a try – I think you'll like it.

This week's feature article by
Thomas W Shinder M.D., etc.
Net Admin Weekly Author

Q & A

Question: Security for Outbound DNS Queries?

to top

Question:

Hi Dr. Tom,

I'm setting up an Internet connection on a small business network that has one Win2k server acting only as a file server, and 13 workstations. There is no DHCP or DNS set up on the network and name resolution is purely NetBIOS (LMHOSTS). I purchased a Netscreen firewall/router that will be connected to the cable modem when it gets installed. The Netscreen works as a DHCP server. There will only be four computers accessing the Internet from the network. I'm concerned about security regarding DNS queries to the Internet. If the workstations on the inside of the firewall are receiving name resolution from outside, I'm worried

about this being a security breach. Does anyone have any ideas how I can set this up with the existing equipment to get a more secure network? Or are my concerns not justified? Any help would be much appreciated. –Worried DNS

Answer:

Hey Worried, don't be so worried. Sounds like you have things under control and you don't have to be so concerned about the security implications of outbound DNS queries. Since your office is very small, it's unlikely that foreign spies are sniffing your wires to determine what Web sites you're visiting. I would think differently if you were running a CIA field office. But regardless of the level of security you require, all DNS queries for public resources are sent in the clear. Public DNS servers can't negotiate security with your clients, so you just have to take the risk that someone will listen in on your queries. However, this information probably won't be very interesting to intruders, unless the intruder is a PI working for a divorce attorney . The situation would be a bit different if you were hosting your public DNS server on your office network. In that case, I would recommend you create a split DNS so that you don't use the same server for advertising your public resources and for resolving Internet host names.

Finally, you shouldn't need to use an LMHOSTS file on a small single segment network. NetBIOS over TCP/IP broadcast traffic shouldn't cause many problems, although you can easily put a WINS server on your Windows 2000 Server. While you're at it, you should also install a DHCP and DNS server on that Windows 2000 Server and relegate your "black box" to firewall and NAT functions.

Running NAT on a Windows 2000 VPN Server

to top

Question:

Dear Dr. Tom,
IAccording to Microsoft Q article 256644, I can install Remote Access and Routing with both NAT and VPN support. Is this correct? I am attempting to make the server function as a NAT and a VPN server, however, I haven't been successful. Any suggestions welcomed... Thanks –Cody

Answer:

Good news for you Cody – there's no problem at all running a NAT and VPN server on the same machine. The Routing and Remote Access Service (RRAS) is installed on Windows 2000 Servers by default. All you need to do is enable RRAS, then install and configure the NAT protocol to make it a NAT server. The VPN server is a bit more complicated. Microsoft has a lot of information on getting your VPN server up and running over at www.microsoft.com/vpn. You can even use the RRAS Wizard to set up the VPN server when you enable RRAS. Be careful about address assignment to the VPN clients. You can use an internal DHCP server to assign IP addressing information to the VPN clients, or you can use a static address pool. If you're not comfortable setting up VPN servers, use a static address pool. You can always switch to DHCP later.

Make sure that you configure RRAS to use the internal interface of the RRAS server to assign WINS and DNS server addresses. The VPN server will try to determine the best choice, but it's best that you double check the setting and configure it yourself. Try using PPTP clients first. PPTP doesn't require a certificate infrastructure and works right out of the box. Finally, confirm with your ISP that they allow incoming VPN connections to your public IP address.

Security Advisories

Cumulative Patch for Internet Explorer

to top

Time to update your Internet Explorer. This latest IE cumulative patch for Internet Explorer includes all the fixes needed to bring you up to date as of November 20, 2002. Check out the site for the specific fixes included in this patch.

Read more...

Attack Targets .info Domain System

to top

This is the second major attack against root DNS in a month. Not good news, but it's good practice. The more of these attacks they see, the faster they learn to respond to the attack. We'll probably see more of these as time goes by, and I expect some increased redundancy to the public DNS in the coming months.

Read more...

Is Linux Really More Secure Than Windows?

to top

Good question. Linux has historically been considered more secure, but there are reasons to think the tide will turn. Microsoft has a new overarching security initiative. If Microsoft does to security what they did with the Internet, we can expect future Windows to be virtually impenetrable. Another Linux security concern is its increased popularity. Linux will become more exposed as more and more shops move away from Microsoft because of egregious licensing. None of this bodes well for the future of Linux as the "more secure" alternative.

Read more...

News Headlines and Resources

What is the Future of Online Training?

to top

It was only a couple of years ago when you heard that classroom training was dead and all training would be online. Well, they were half right, classroom training is dead, but then so is all training! Well, not exactly, but things didn't quite pan out how we expected. Check out this very interesting article about the evolution of online training and see if it might be in your future.

Read more...

Multiple SMTP Virtual Servers Issue

to top

Here's a problem we ran into last week. We had several virtual SMTP servers on the same Exchange server and we needed each server to show a different host name in the service banner. Sounds easy, and it is! Check out the KB article for the details.

Read more...

Intel Guide to Home Network Security

to top

Here's a nice article on network security that focuses on smaller environments. The network could be a home network, a SOHO, or even an SMB (small/medium-sized business). The principles remain the same. They say that all politics are local politics; in the same way, large networks are just a collection of small networks. Nicely written article by the folks at Intel.

Read more...

Microsoft Security Response Center Rating System

to top

If you've been following the security updates in this newsletter, you know that it's sometimes hard to figure out how severe the threat might be. Microsoft has fixed this problem and now provides a simplified threat reporting mechanism. Check out the full article for details.

Read more...

Wireless Email with Mobile Information Server 2000

to top

Do you have an Exchange Server? Want to connect your wireless PocketPC2002 devices to that server? You could use Blackberry, but why not try a home-grown solution instead? Mobile Information Server 2002 and PocketPC go great together! Throw ISA Server 2000 into the mix, and you have a secure and reliable email access solution for Microsoft PDAs.

Read more...

Network File Errors and Windows XP SP1

to top

Are you experiencing connection problems between Windows XP and Windows 2000 computers after upgrading to Windows XP SP1? Well, join the club! There are differences between how Windows XP and Windows 2000 perform SMB signing. If you have connectivity problems between your XP and 2K machines, then you should definitely check out this article ASAP.

Read more...

Support WebCast - Maintaining Your Windows XP System

to top

This Support WebCast session will examine some of the best practices you can use to keep your Microsoft Windows XP system up-to-date and make sure it runs smoothly. They'll also cover techniques you can use for easy recovery. Specific topics will include Backup and Automatic

System Recovery, System Restore, antivirus products, firewalls, Windows Update, and Automatic Updates.

Read more...

Download of the Week

TweakSEC

to top

You've been around the block a few times and you know computer security is more art than science. There's no "right way" to do it, and it's all related to your risk tolerance. There are about a million (estimated) different security-related settings on a Windows computer. Which ones should you set? Why? How? Help! Check out TweakSEC. It's a security configuration and administration tool that's easy and fun to use. Use the program to explore the various Windows security settings and then manipulate settings to learn how increased "security" often results in a self-imposed DoS attack! Free trial download here.

Read more...

Free Cramsession IT Newsletters - Choose Your Topics!

H = HTML Format **T** = Text Format

H	T		H	T		H	T	
☐	☐	A+ Weekly	•	☐	Exam Tips 'N Tricks	☐	•	.NET Insider
☐	•	ByteBack!	☐	•	IT Career Tips	•	☐	Script Shots
☐	☐	Cisco Insider	•	☐	Linux News	☐	☐	Security Insider
☐	☐	Developers Digest	☐	•	Must Know News	•	☐	Trainers News

Enter your Email

Subscribe Now!

CramSession
Prepare for Success!

Your subscribed e-mail address is:steven.thode@toadworld.net
To unsubscribe, simply **click here** and hit "send" in your e-mail reader.