Windows Insider
35,000 Subscribers Worldwide
May 8, 2002
Issue #91

Feature

What's New in .NET Server VPN Support Read it

Ask Uncle Bill

Q and A's Read it

Security Advisories

No New Security Advisories for this Week Read it

News Headlines & Resources

How Infrared Devices Work Read it
Hosting a Web Site from Home Read it
What's New in .NET Server? Read it
Will StarOffice Eat into MS Office's Market Share? Read it
NIST Internet Time Servers Read it
Cool Lightweight Packet Sniffer for Windows 2000/XP Read it
Are Things Ever Going to get Better? Read it
Windows XP Baseline Security Checklist Read it
Using ISA Server for Advanced Authentication and Authorization Read it
Microsoft Exchange: Offline Defragmentation with the Eseutil Utility Read it

Download of the Week

Pest Patrol Read it

Feature

What's New in .NET Server VPN Support

to top

VPNs are cool, no doubt about it. You don't really appreciate VPNs until you start to travel. Once you hit the road and realize that you've left some "must have" information on the file server on the corporate network, you'll realize just how cool, and what a lifesaver, a VPN network connection can be.

Although VPNs are hardly new, they just seem to get more and more popular. The reason for this might be that corporations, large and small, finally realize they can dump their expensive dial-up setups and put in a VPN solution for a fraction of the cost. They also realize that you can leverage an existing Windows 2000 Server installation to create a VPN server without buying more licenses just for VPN connections. Contrast this policy with the likes of Checkpoint!

Like Windows 2000, .NET Server supports both PPTP and L2TP/ IPSec for VPN clients and servers. You can create VPN servers that accept calls from VPN clients and you can create VPN gateways to connect disparate networks. But, .NET Server adds some extra features that makes working with VPNs even easier and more secure.

NetBIOS Proxy

If you hang out in the RAS/Networking newsgroups and other Internet forums dedicated to discussions on Windows 2000 RAS networking issues, you'll have noticed one of the most common questions on the boards is "Why can't I connect to my computers on the remote network?". After drilling down a bit, you realize the issue is usually a name resolution problem, not a connection problem.

VPN clients can use either DNS or WINS to resolve names for hosts on the remote network. DNS is the preferred method, but many networks still run NetBIOS-dependent applications or services (such as the dreaded browser service) and therefore need WINS servers. Windows 2000/.NET VPN servers can be configured to assign name server addresses to VPN clients based on the WINS/DNS configuration on one of the internal interfaces of the VPN server, or you can use a DHCP Relay Agent on the VPN server to assign alternate WINS/DNS server addresses to the VPN clients.

Smaller networks might not want or need to implement WINS or DNS for host name resolution. Small, single segment networks can use NetBIOS broadcasts to resolve names on the local network by using NetBT (NetBIOS over TCP/IP). If you're using a Windows 2000 VPN server, your only choice is to use a HOSTS or LMHOSTS file on the VPN client to resolve names on the remote network.

.NET Server solves this problem by implementing a new feature: the NetBT Name Resolution Proxy. Here's how it works:

1. When the VPN client needs to resolve a name on the remote network, The client broadcasts a NetBIOS Name Query Request which is received by the VPN server.

2. The VPN server checks its local NetBIOS name cache to see if it already contains a mapping for the host. If there is no entry in the cache for sought after host, the VPN server broadcasts on all

interfaces a NetBIOS Name Query Request; this includes the VPN interface.

3. The NetBIOS host on the remote network responds to the VPN server's NetBIOS Name Query Request with a positive NetBIOS Name Query Response message.

4. The VPN server receives the positive NetBIOS Name Query Response and puts the NetBIOS name/IP address mapping in its local NetBIOS name cache. It then forwards the positive NetBIOS Name Query Response message to the interface that issued the request, which in this case is the VPN interface.

5. The VPN client receives the IP address mapping for the NetBIOS host and sends a request to the IP address of NetBIOS host on the remote network through the VPN interface.

This feature won't be such a big deal to those of you running enterprise networks, but the small business or corporate remote office will be a lot easier to access with this new feature in place.

Pre-shared Key for L2TP/IPSec Connections

One thing that keeps most people from using L2TP/IPSec for their VPN protocol is the need to deploy machine certificates on their VPN servers and clients. If you ever tried to put together a large scale (or even small scale) certificate server/PKI solution, you know that it's no fun, and can be rather complex.

.NET Server allows you to use a pre-shared key instead of a machine certificate. That's right! Neither the .NET VPN server nor the VPN client needs a machine certificate installed to create an L2TP/IPSec VPN link. One drawback here is that you need to use Windows XP for your VPN client. Other Windows VPN clients do not support the pre-shared key arrangement, so those clients will need a machine certificate installed.

While pre-shared keys make things a bit easier, they aren't the most secure solution. You're better off using the pre-shared key approach only until you've had the chance to complete your certificate server/PKI deployment.

A place where pre-shared keys may be popular is when you want to join networks using VPN gateways. You might have no interest in creating a PKI for your organization and you're happy using PPTP for your VPN clients. However, you would like to use IPSec to join your VPN gateways. In this case, you can implement L2TP/IPSec gateway-to-gateway tunnels between your VPN servers.

IPSec through NAT Servers

Most networks are protected by firewalls of one kind or another. Most firewall implementations also integrate NAT functionality when they provide a gateway to the Internet. Internet network clients behind the NAT server can make PPTP connections to VPN servers on the Internet. If you want to use L2TP/IPSec through the NAT server, you're out of luck.

In L2TP over IPSec, the UDP and TCP headers contain a checksum that is

based in part on the source and destination IP address of the IP header. The addresses in the clear IP header cannot be changed without invalidating the checksum in the TCP and UDP headers. Even if you could somehow update the checksums and not invalidate the packet, the TCP and UDP checksums cannot be updated because they are within the encrypted portion of the ESP payload.

However, .NET Server allows you to pass L2TP/IPSec packets if IPSec uses only ESP and not AH. The IKE protocol will detect the presence of NAT and add UDP port 500 header to the IPSec ESP traffic. When the UDP port 500 traffic hits the VPN server that recognizes the IPSec UDP encapsulation, the VPN server will be able to unwrap the packet and decrypt the IPSec protected contents. Success depends on both the VPN client and server being aware of the UDP encapsulation of IPSec ESP packets. For more information on the spec, click here.

You can use this setup when VPN clients want to make L2TP/ IPSec connections through the NAT server to clients on the Internet. But, you can also use it to securely connect to clients on a DMZ segment. I run into many administrators who want to do terrible things such as allowing SMB communications through their firewalls to access machines on their DMZ segments. With .NET Server, you can use a L2TP/IPSec tunnel to securely connect to the DMZ hosts without badly violating your internal network's security zone.

Summary

.NET Server adds some cool features to an already great Windows 2000 VPN implementation. The most useful new feature is the ability to pass L2TP/IPSec through the NAT server. This feature can be combined with the new and improved .NET Server Network Load Balancing to give you a powerful, secure and fault tolerance VPN client/server solution.

This week's feature article by
Thomas W. Shinder,
M.D., MCSE

Ask Uncle Bill

Q and A's

to top

Question:

Hi, Uncle Bill.
Hello there! I'm having trouble with the system log on the event viewer (Win2k). It's piling up with Event I.D. 5775. DNS deregistrations are occurring and I haven't a clue! Perhaps someone could shed some light on this issue for me. Thanks a bunch! I look forward to a response.
--Jeff

Uncle Bill says:

Hey Jeff! That's a pretty weird problem you're having. However, I went to www.eventid.net and found some information on this error. Here's what they had to say:

"In general, these error messages are logged because the Netlogon

service does not receive a "success" message from the DNS server that owns the zones of the records that are being registered."

For more info, click here and click here.

Question:

Hi, Uncle Bill
How do I delegate the power to Unlock locked accounts? I understand the Delegation Wizard but nowhere does it say "delegate the authority to group x to allow them to unlock locked accounts". Thanks for you input
--Mike

Uncle Bill says:

Yo Mikey! No problem! Here's how I found the solution. Crack open that TechNet CD you have lying around somewhere in your office. Open up TechNet, press CTRL+D and type in: "unlock near delegate" (without the quotes). The TechNet CD search engine will look for where the words "unlock" and "delegate" are near each other. I came up with two articles and Q294952 looks like the best one for you.

Don't Be Shy!

Got a question about MCSE certification or an event log error that just won't go away? Send it in! We'll be answering a question or two every week. Send your submissions to Uncle Bill **here**.

Security Advisories

No New Security Advisories for this Week

to top

No new security advisories for this week. Time to take a breather, review your current security policies, and audit your servers for security weaknesses.

News Headlines and Resources

How Infrared Devices Work

to top

Have you ever used the cool IR interface in Windows 2000/XP? If not, you should give it a try sometime. If you have used the IR interface, you know how cool it is. But, do you know how IR technology works? If not, take in this excellent review of IR connections.

Read more...

Hosting a Web Site from Home

to top

You'll need to have a good understanding of how Web servers work on the Internet if you're studying for your Windows 2000 MCSE exams. Have you set up a live Web server yet? If not, there's no time like the present! Check out this article to get a leg up on hosting your own Web services.

Read more...

What's New in .NET Server?

to top

Windows 2000 is going to be a tough act to follow. What does Window .NET Server offer that Windows 2000 does not? Check out this site for a detailed rundown of what's new and improved.

Read more...

Will StarOffice Eat into MS Office's Market Share?

to top

The Gartner Group suggests that Sun's StarOffice suite of productivity applications may garner as much as 10% market share by 2004. Makes sense, as they have versions for Windows, Linux and Solaris. An organization can easily standardize on this low cost alternative, and it would make it easier for all users to migrate to a new platform entirely.

Read more...

NIST Internet Time Servers

to top

Keeping accurate time on your network is important for a lot of reasons, not the least of which is making sure your Active Directory infrastructure stays in good shape. Here's a list of time servers run by NIST that you can use to synchronize your network.

Read more...

Cool Lightweight Packet Sniffer for Windows 2000/XP

to top

How about a free lightweight sniffer that doesn't require you to install any drivers that might muck up your TCP/IP stack? Don't think there is such a thing? Wrong! This sniffer works well on both Windows 2000 and Windows XP. It can import from (and export) NetMon .cap files too.

Read more...

Are Things Ever Going to get Better?

to top

We all know that we're going through some hard times in the IT employment market right now. But will things ever get better? Will they ever reach what they were back in the good old days of the 1990's? Check out this article and compare what you think with the author's opinion.

Read more...

Windows XP Baseline Security Checklist

to top

Are you thinking about rolling out Windows XP in your office? If so, you should be thinking about what measures you should take to secure these boxes. Microsoft provides a nice checklist to help you in your task.

Read more...

Using ISA Server for Advanced Authentication and Authorization

to top

Check out how ISA Server can help you with advanced authentication and authorization. See how you can authenticate with the Web server, the ISA Server or both! Excellent presentation from the MEC 2001.

Read more...

Microsoft Exchange: Offline Defragmentation w/Eseutil Utility

to top

Is your Exchange Server getting a bit pokey? Are users calling you to complain that it takes a long time to delete email and move from folder to folder? You might need an offline defrag of your message store. Check out this online seminar for all the details.

Read more...

Download of the Week

Pest Patrol

to top

Spyware and Scumware is proliferating on the Internet. Do you know what hidden programs and back doors have been installed on your computer? How about evil cookies? If not, you need some kind of digital bug spray to kill those nasty things! Pest Patrol does the job! You can download an eval version, and if you find pests, the full version only cost $19.95US (which will let you whack the pests!).

Read more...

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,
or visit the **CramSession Unsubscribe Page** .