Steven Thode

From: CramSession [listboss@list.cramsession.com]
Sent: Thursday, May 29, 2003 1:46 AM
To: Steven Thode
Subject: Net Admin Weekly - Issue 32

Net Admin Weekly

59,000 Subscribers Worldwide

May 29, 2003
Issue #32

CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters CramSession

Feature

What's New and Cool in Windows Server 2003 VPN Networking Read it

Q & A

DNS Forwarders Don't All Forward Read it
When to Superscope? Read it

Security Advisories

Flaw in Windows Media Player Skins Downloading could allow Code Execution (817787) Read it
Information on Bogus Microsoft Security Bulletin E-mails Read it
Windows Server 2003 Threats and Countermeasures Guide Read it

News Headlines & Resources

First Windows 2003 Core Exams Get Tested Read it
The Details of the Windows XP System Restore Read it
How to Troubleshoot TCP/IP Connectivity in Windows XP Read it
Microsoft Product Support's Customer Configuration Capture Tools Read it
Microsoft Windows 2000 Security Hardening Guide Read it
Inside the UrlScan 2.5 Security Tool Read it
Support WebCast: Microsoft Exchange Server 2003: An Overview of the New Administration Features Read it

Download of the Week

L2TP/IPSec NAT-T Update for Windows XP and Windows 2000 Read it

Feature

Feature: What's New and Cool in Windows Server 2003 VPN Networking

to top

One question that I hear a lot of is “why should I upgrade from Windows 2000 to Windows Server 2003?” That’s a good question. While the decision to upgrade from Windows NT 4.0 to Windows Server 2003 is a no-brainer, the cut gets a little finer when trying to figure out whether you should pony up the big bucks to get what many people consider a “point one” upgrade.

Whether you make the upgrade not depends on general characteristics of the operating system and specific features the operating system provides that adds value to your business. General characteristic of Windows Server 2003 that everyone benefits from include:

- Most secure Windows OS ever released
- Most stable Windows OS ever released
- Best documented Windows OS ever released
- Best supported Windows OS ever released

While these general characteristics are fine, they’re really not enough to make me put my hand in my pocket and hand over the bucks to Microsoft for the upgrade. What I need is a value add that excites me, and which keys into how I use Windows every day.

That’s where the VPN improvements come in. With the price of hardware coming down so much, and the cost of Windows Server 2003 remaining stable compared to previous versions of Windows, I see the Windows-based VPN server as what we used to call “a high-value proposition”. Windows 2000 VPNs were easy to configure, allowed me to create VPN servers and VPN gateways, and supported very high encryption, smart cards, and certificate authentication (even using the built in Certificate Server that comes with Windows). While I could pay license fees to 3rd party VPN box builders, I’d rather pay those fees to IPSec NIC vendors to improve the performance of my L2TP/IPSec connections with encryption offloading.

So what’s new with Windows Server 2003 VPN networking? Check this out:

- Full support for Network Load Balancing (NLB)

- NetBIOS over TCP/IP (NetBT) name resolution proxy
- Support for pre-shared keys for L2TP/IPSec connections
- Support for IPSec NAT Traversal

Full Support for Network Load Balancing (NLB)

One of the main problems with providing load balancing and fault tolerance for VPN connections in Windows 2000 was that NLB was supported on a single interface. In order to provide full fault tolerance and load balancing for VPN links, you need network load balancing on both the internal and external interfaces of the VPN Server. Windows Server 2003 allows you to bind the NLB protocol to both the internal and external interfaces.

Another significant improvement with Windows Server 2003 is that now you can use L2TP/IPSec in a network load balancing environment. In Windows Server 2003, you could not use L2TP/IPSec in a NLB configuration because of problems with rebalancing sessions when servers are added or subtracted, which is related to the fact that L2TP uses UDP for its control and tunnel maintenance channel.

One of the biggest bugaboos with NLB and VPN was seen when multiple addresses were bound to the external interface. If the VPN link was created to one of the secondary addresses, the response always came back via the primary addresses. This breaks most VPN clients connections. Windows Server 2003 fixes the problem which also allow both PPTP and L2TP/IPSec VPN connections to work flawlessly with the Windows Server 2003 VPN Server.

NetBIOS over TCP/IP (NetBT) Name Resolution Proxy

SOHO and small business offices with a single Windows Server 2003 Server will benefit from the NetBIOS over TCP/IP (NetBT) name resolution proxy feature. In these small environments you might not want to incur the administrative overhead of installing a WINS server, especially if you have to put that WINS server on a multihomed domain controller that's connected to the Internet.

A far better solution would be to allow the VPN server to forward NetBIOS name resolution request to segments that are directly connected to the VPN server. When a NetBIOS host responds to the request, then the VPN server hears the response and forwards the answer to the VPN client that made the request for resources on the NetBIOS host.

The key here is that the VPN clients don't depend on a working WINS or DNS infrastructure in order to connect to resources on the internal network by name. Just this feature will reduce the number of support calls about not being able to connect to NetBIOS dependent resources on the internal network behind the VPN server.

Support for Pre-shared Keys for L2TP/IPSec Connections

One of the main barriers to entry when it comes to rolling out a L2TP/IPSec VPN infrastructure is the requirement for a Public Key Infrastructure. This includes creating certificate servers and assigning certificates to VPN clients. The whole PKI thing has a significant learning curve and busy network admins don't always have the time to ramp up on PKI, certificate servers and certificate assignments.

You can still have the link security provided by L2TP/IPSec and not use certificates. In Windows Server 2003, you can use a pre-shared key. You assign a pre-shared key to the VPN server and VPN client and the client and server will use the shared secret to create the secure channel. Pre-shared keys suffer from not being very scalable, but they work fairly well in a smaller environment or as a stop-gap measure while preparing your Public Key Infrastrucuture.

Support for IPSec NAT Traversal

I've written about the problems with getting IPSec based communications through a NAT. Address translation breaks the authentication scheme used by IPSec, so you can't use IPSec ESP when a NAT device is in the path between a client and server. This means if you have a L2TP/IPSec client on your internal network behind a NAT server, you will have to use PPTP, because L2TP/IPSec just won't work.

Windows Server 2003 changes this. When you use a Windows Server 2003 VPN Server, it can recognize when the L2TP/IPSec client is behind a NAT device and accept packets that are encapsulated in a specific UDP header. The Windows Server 2003 NAT Traversal mechanism is based on RFC draft standards and will be implemented on all network devices in the near future. The Windows Server 2003 VPN server listeners on UDP port 4500 and takes the UDP header off and expose the IPSec packet. This is how NAT-T works, its wraps the ESP protected packet with a UDP header. Its this encapsulation that allows communications to go through the NAT server without breaking IPSec.

There are now VPN client updates for Windows 9x, Windows 2000 and Windows XP that allow these clients to use NAT-T. The new VPN client software allows these clients to use UDP encapsulation when they detect they are behind a NAT device. Bottom line: you don't have to worry about your Windows based VPN clients having problems connecting to your Windows Server 2003 VPN server when those clients are behind a NAT. You can find the new LT2P/IP-Sec NAT-T clients for Windows XP and Windows 2000 **here**. You can also find the client, along some additional information **here**.

Conclusion

The VPN server improvements included with Windows Server 2003 are enough to encourage me to upgrade. While the new features are nice, even nicer is the improved stability and reliably of the Windows Server

2003 VPN server. We used to have line dropouts for no apparent reason with Windows Server 2003. I never see these anymore with Windows Server 2003! Give Windows Server 2003 a try and let me know what you think of the VPN enhancements. Thanks! –Tom.

Thomas W Shinder, .Net Admin bi-Weekly Editor
Co-Author, **Configuring ISA Server 2000**
Co-Author, **ISA Server and Beyond**

Q & A

DNS Forwarders Don't All Forward

to top

Question:

Hi Dr. Tom,

I have a DNS server (10.0.0.3) that has forwarding set up to work with a external DNS. I can do an NSLOOKUP for www.cnn.com and get the info back, so I know that I can get out and am correctly forwarding requests to my external DNS. What I have set up now is a second forwarder so that I have two externals listed in the forwarding tab. Here's where it gets weird. I should be able to have the first external DNS go offline and still send my forward requests to the second external, but that's not happening. I'm getting unresolved when I take that first external server down. It's like the 10.0.0.3 DNS isn't realizing that it has a second forwarder in the tab. Basically I think it's giving up after trying the first forwarding server and not even attempting to go to the other option. -- ND

Answer:

Hey ND, great question! As you know, a forward is a DNS server that can resolve names for a DNS server when the DNS server is not authoritative for the domain it's trying to resolve. When you use a forwarder, you are letting another DNS server resolve the name and then forward the results back to your computer. If the forwarder can't resolve the name, the DNS server that sent the request to the forwarder can try to resolve the name itself by performing recursion (with the aid of the Root Hints file on that DNS server). I suspect your DNS server is actually performing recursion itself and never sends the request to the forwarder. This happens when you disable recursion from the Advanced tab of the Zone properties dialog box. Enable recursion again and the DNS server will be able to use all forwarders on your list.

When to Superscope?

to top

Question:

Dear Dr. Tom,

I have my 216 on Friday but am confused with DHCP Superscopes and when to use them; I have read Thomas W Shinder article in the additional links of this web site, which I used to base my answers to my "Self Test" practice software, but it is telling me my answer is not correct. The question goes like this; Multiple subnets connected by BOOTP routable routers. One DHCP server on 1 subnet configured with multiple scopes, servicing all the subnets. My answer follows the line of "this will NOT work, must use a Superscope" - but it's wrong. The self test software says this is a perfectly correct set -up. But surely, as far as the DHCP server is concerned, it's listening to just one big subnet on a single NIC, so it will check its own NIC subnet, against the incomming DHCP requests from the clients, see most of them don't match the subnet it's on, check for a Superscope, not find one, then say, no sorry, can't help! - can you help? Is my Self test software wrong? –Russell Cox

Answer:

Hey Russell, thanks for reading my stuff! The key to the superscope issue is that you need to be supporting multinets to use the superscope. The multinet can be directly connected to the DHCP server, or it can be on a remote subnet and the packets are passed via a router performing BOOTP forwarding or a DHCP relay agent. There are three circumstances where you would use a superscope:

- When the address pool for a active scope is nearly used up, and you need to add more computers to the network. You need to use another IP network range of addresses to extend the address space for the same physical network segment.
- Clients must be migrated over time to a new scope (such as to renumber the current IP network from an address range used in an existing active scope to a new scope that contains another IP network range of addresses).
- You want to use two DHCP servers on the same physical network segment to manage separate logical IP networks.

In each of these circumstances, you configure multiple network IDs on the same physical segment (same broadcast domain). That's what creates the multinet. If you want to support DHCP on a multinet, then you need to configure a superscope.

Security Advisories

Flaw in Windows Media Player Skins Downloading could allow Code Execution (817787)

to top

A flaw exists in the way Windows Media Player 7.1 and Windows Media Player for Windows XP handles the download of Media

Player skin files. The flaw means that an attacker could force a file masquerading as a skin file into a known location on a user's machine. This could allow an attacker to place a malicious executable on the system.

Read more...

Information on Bogus Microsoft Security Bulletin E-mails

to top

Have you been getting a lot of email from support at Microsoft dot com? If so, you should know that it's not from Microsoft. Neither are those security alerts you've been getting that have attached files. Check out this link to find out what Microsoft official policies are regarding alerts and patches.

Read more...

Windows Server 2003 Threats and Countermeasures Guide

to top

We've posted the link to the Windows Server 2003 Security Guide in a previous edition of this newsletter. Now you need to get its companion Threats and Countermeasures Guide. There are chapters on System Services, the Event Log, Member Server Hardening Procedures and a lot more. Put this guide on your "must have" list.

Read more...

News Headlines and Resources

First Windows 2003 Core Exams Get Tested

to top

Thinking about upgrading your MCSE to Windows Server 2003? Windows Server 2003 is the most polished, most secure, most intuitive and sophisticated Windows operating system ever released. Even if you don't need a Windows Server 2003 MCSE, I think you'll have fun studying for it! No lie. The help files are great and the entire interface and underpinnings are extensive documented.

Read more...

The Details of the Windows XP System Restore

to top

Ever wonder what System Restore is watching for? Me too. Then check out this page that has the details on what the System Restore feature is monitoring and how it monitors those things it monitors.

Read more...

How to Troubleshoot TCP/IP Connectivity in Windows XP

to top

Troubleshooting TCP/IP connections is a daily task around here. There are several ways to troubleshoot TCP/IP, unfortunately the most

common one is to restart the computer! Check out this article for some good tips and tricks on how to use a Windows XP machine to help troubleshooting TCP/IP connectivity issues.

Read more...

Microsoft Product Support's Customer Configuration Capture Tools

to top

Here's a collection of invaluable tools from Microsoft PSS that can document just about any component of a Windows NT 4.0, Windows 2000 or Windows XP operating system. There are multiple downloads, so pick the one you need and get that one first.

Read more...

Microsoft Windows 2000 Security Hardening Guide

to top

You've got Security Guides, Threat Guides, Config guides and user guides. Now try this one: the Windows 2000 Security Hardening Guide. You can't have too many guides! Or can you? <g>. This one is pretty good, just be careful you don't DoS yourself.

Read more...

Inside the UrlScan 2.5 Security Tool

to top

Check out the new features found in URLScan 2.5. Now you can change the log file directory, log long URLs, and restrict the size of requests. You can also check out whether you should install URLScan on an IIS 6.0 server. You might find the answer very interesting!

Read more...

Support WebCast: Microsoft Exchange Server 2003: An Overview of the New Administration Features

to top

Exchange 2003 is almost out the door and let me tell you something, its really cool! The new OWA is a must have feature. If you plan to install Exchange on Windows Server 2003, then you're going to need to upgrade to Exchange 2003. This WebCast will go over inside info on the new admin features you'll see with Exchange 2003.

Read more...

Download of the Week

Download of the Week – L2TP/IPSec NAT-T Update for Windows XP and Windows 2000

to top

Have you been going crazy trying to get your L2TP/IPSec clients connected to external VPN servers on the Internet through your NAT based firewall? Me too! Well, if your problems were with Windows XP and Windows 2000 worry no more. All you need to do is allow outbound UDP 500 and UDP 4500 and let 'er rip. The IPSec ESP packets are encapsulated in a UDP header, so now you can pass them through the NAT. Check the link for more info and a download.

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.