Net Admin Weekly
53,000 Subscribers Worldwide
November 13, 2002
Issue #17

Feature

VPN Clients and Split Tunneling Read it

Q & A

Why WINS? Read it

Accessing Exchange from the Internet Read it

Security Advisories

Cumulative Patch for Internet Information Service Read it

Cumulative Update for Outlook Express 6.0 SP1 Read it

AntiOnline Employment Opportunity - Spy on Users for Fun and Profit Read it

News Headlines & Resources

NetWare 4 to NetWare 6 CNE Upgrade Read it

It's Official: No Longhorn Server On Tap Read it

Windows XP Defrag Utility Command Line Reference Read it

Crypto for VPNs Q and A Read it

101 Things that Mozilla can do that IE Cannot Read it

How to Become a Microsoft Beta Tester Read it

Safeguard Windows 2000 Terminal Servers from Attack Read it

Download of the Week

FolderMon Read it

Feature

VPN Clients and Split Tunneling

to top

Chances are you're in the process of rolling out a new VPN client server setup, or you're already managing one. Windows 2000 VPNs are fun to design and configure because there are so many options available. Spoke and Hub or Mesh? PPTP or L2TP/IPSec? VPN Server or VPN Gateway? Policy via user account or RAS Policy? What's really great is configuring VPN client/ server setups are easy, in spite of the fact you have so many options.

I was talking to a friend yesterday about a VPN he was setting up. He was very excited about the whole thing and spent over an hour telling me each and every detail of his design. During a breathless moment at the end of his story, I asked him if he planned to disable split tunneling for his VPN clients. He gave me a cross-eyed look and finally asked "what's split tunneling?"

What are you supposed to do when you haven't heard of something? Hit the TechNet CD! So we went to a computer with a TechNet CD on it and searched for "split tunneling". No results. Then we tried "split tunnel". Still nothing. Then we tried "'split' near 'tunnel'". Still nothing. No wonder my friend had never heard of split tunneling. Clearly no one at Microsoft had heard of it either!

You can run into some real security problems with VPNs that allow split tunneling. The problem centers around VPN client configuration. The default Microsoft VPN client configuration is secure. That's because the default Microsoft VPN client configuration does NOT allow split tunneling. You only run into problems when you change the default setting. Sometimes you need to make this change, and sometimes the change is made to subvert network security.

Now what is this mysterious setting I'm talking about? It's the "Use default gateway on remote network" Option on the VPN client. This option appears in various places, depending on the version of Microsoft VPN client you're using. On a Windows XP Pro Computer, you'll find it this way:

1. Right click the My Network Places icon on the desktop and click Properties.
2. Right click on your VPN client connections in the Network Connections window and click Properties.
3. Click the Networking tab, and then click on the Internet Protocol (TCP/IP) entry and click the Properties button.
4. On the General tab of the Internet Protocol (TCP/IP) Properties dialog box, click the Advanced button.
5. On the General tab of the Advanced TCP/IP Settings dialog box, note the "Use Default Gateway on Remote Network" option.

This is a significant setting. It makes the difference between a secure VPN client connection, and VPN clients that are hacker, virus, and worm gateways.

VPN Client Default Route

The "Use Default Gateway on the Remote Network" option is enabled by default. When the VPN client connects to the VPN server, a new default route is created on the VPN client and it appears in the VPN client's routing table. You can view this new route by opening a command prompt and typing the "route print" command. The new default route replaces the old default gateway that was set on the VPN client when the initial dial-up connection was established (assuming the VPN client connected to the ISP via a modem). The default gateway is set as the ISP's router when a dial-up connection is used. This allows the dial-up clients to access the Internet.

A VPN client with the "Use Default Gateway on Remote Network" setting enabled cannot access the Internet because the VPN client now uses the VPN interface to route packets to remote (non-local) networks after the new default route is added. Since all networks except for those on the network ID assigned by the ISP to the modem interface are non-local, all packets are forwarded to the VPN server through the client's VPN interface.

This is exactly what you want. You do not want VPN clients accessing your private network *and* the Internet at the same time. Allowing a VPN client to directly access the Internet and your internal network at the same time is like spraying nerve gas on your network security infrastructure. The reason for this is that the VPN client can become a gateway between the Internet and your private network.

You have a split tunnel configuration when you allow clients to connect the VPN and the Internet at the same time. Split tunneling is enabled when the "Use Default Gateway on Remote Network" option is *disabled* for the VPN interface. Now you understand why split tunneling can be so toxic to network security.

While this is the best configuration for you and your network's security, it can lead to many Help Desk calls. VPN users may complain that they can't surf to porno sites, connect to AOL "cyber" rooms, use Kazaa, Morpheus, or other virus/worm download services, or any of the other unsavory activities that you have dutifully prevented them from doing when they are directly connected to the internal network and are subject to your firewall policies.

How to Beat Down Users who Disable the Default Gateway Setting

You run into big trouble when users decide to subvert network security by disabling the "Use Default Gateway on Remote Network" option. When users disable this option, a network route is still added to the VPN client's routing table, but it is not a default route. Instead of adding a new default route (gateway), the route added directs requests for the classfull network ID the VPN client was assigned on its VPN interface. Since the default route continues to be the ISP's remote router, the VPN client can still directly connect to resources on the Internet.

For example, when a VPN client is assigned the address 10.0.1.100, a route for network ID 10.0.0.0/8 is set. All packets for that network ID

(and all subnets of that network ID) are sent to the VPN server. All other non-local packets are sent to the ISP's remote router. The VPN client now has a direct link to the Internet AND the corporate network, and can become a gateway between the Internet and the corporate network. From a network security point of view, things can't get much worse.

There are ways to prevent users from changing the gateway setting. The Connection Manager Administration Kit allows you to create VPN connectoids, and there may be a feature that allows you to prevent users from changing this option. I know that on a Windows XP Professional machine, an administrator can create a VPN connectoid and set the option that it is available to all users. When an average user logs in, they cannot access the Properties dialog box. However, if users configure own VPN connectoids, they will be able to make whatever changes they like to the connectoid.

Improve VPN Client Security with Off-Subnet Addresses

A better way to secure your internal network from rogue users is to design the IP addressing and routing scheme in such as way so that when users set their VPN clients to use split tunneling, they still won't be able to access anything other than resources on the VPN server itself.

You can accomplish this goal by assigning VPN clients "off-subnet" IP addresses. An off-subnet IP address is one that's not on the same network ID as the internal interface of the VPN server.

For example, the internal interface of the VPN server is connected to network ID 10.0.0.0/16 and the VPN clients are assigned IP addresses in the 169.254.0.0/16 range. With this setup, VPN clients configured to not use the VPN server as their default gateway will be able to access resources on the VPN server (split tunneling is enabled), but won't be access to access resources anywhere else on the internal network.

The reason is that when the VPN client is not configured to use the default gateway on the remote network, the actual default gateway on the client points to the ISP (the Internet). Therefore, any non-local requests (including those for network ID 10.0.0.0/16) will be forwarded to the Internet, which won't work because the 10.0.0.0/16 network is a private network ID. Even though the VPN server contains proper routing table entries to forward requests to all the network IDs on the internal network, the off subnet VPN client won't be able to take advantage of them because they are not using the VPN server as their default gateway. So in this case, the VPN client never even tries to send packets for network ID 10.0.0.0/8 to the VPN server. This strikes at the heart of malicious users who try to enable split tunneling!

Another Example of Off-Subnet Addressing Benefits

Here's another example of how off-subnet IP addresses for the VPN clients protects your network. Consider the following:

The VPN client is not configured to use the default gateway on the remote network (split tunneling is enabled). However, the VPN client is

assigned an IP address that is valid on the network ID directly attached to the VPN server's internal interface. Suppose the VPN server is directly attached to network ID 10.0.0.0/16, and the VPN client is assigned the IP address 10.0.0.100/8. Why is the VPN client assigned a different network ID? The reason is VPN clients are always assigned classfull addresses, and the route created on the VPN client is a classfull route.

If you have configured a nice, hierarchical routing infrastructure, your internal network IDs are all subnets of 10.0.0.0/8, with network ID 10.0.0.0/16 at the top of the hierarchy. You'll have a number of subnet IDs, such as 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16 and so on. These are all subnets of the classfull network ID 10.0.0.0/8.

How you would summarize your internal network ID? You would create a route to network ID 10.0.0.0/8, which is exactly what the VPN server does for the VPN client. Even though the VPN client isn't using the VPN server as its default gateway, it doesn't need to. The reason for this is that all of your internal subnets are nicely summarized by the routing table entry created on the VPN client.

If the client needs to get to network ID 10.1.0.0/16, it can because the routing table entry for the VPN interface is valid for routing requests to that network ID through the VPN interface. Now the clients with split tunneling enabled are able to access all network IDs on your internal network because you did a good job summarizing your network.

So, while route summarization is a good thing, it can be your undoing if you don't configure your VPN clients to use an off-subnet IP address.

Summary

Split tunneling is something that doesn't get a single reference in TechNet, but it does represent a real problem in terms of VPN client configuration. You should also enforce a policy that prevents split tunneling for VPN clients. This will help prevent the VPN clients from becoming gateways for viruses, worms, and other malicious code. It's hard enough keeping your network secure without having to worry about VPN clients creating havoc.

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

Q & A

Question: Why WINS?

to top

Question:

Hey Dr. Tom,

I have an NT domain with about 200 nodes. Everything is working fine as far as network traffic and browsing the network. I was wondering why is

it that some people use WINS on their network. I know it helps name resolution on the network, but I'm pretty sure they can browse the network without it. Just a thought that came up in my head. -- ejeangilles

Answer:
Hi EJ! WINS allows your Microsoft WINS clients to dynamically register with the WINS server and query the WINS server for NetBIOS name resolution. If you don't use a WINS server, NetBIOS hosts on your network must either use a LMHOSTS file or NetBIOS broadcasts. If you have 200 hosts on in a single NetBIOS broadcast domain (single IP subnet), you certainly will have a good amount of NetBIOS broadcast traffic occurring. When is the last time you ran a protocol analyzer on your network? You might be surprised by the amount of needless name resolution traffic occurring on your small network. A WINS server can get rid of almost all that traffic and it requires very few system resources. Put the WINS server on your domain controller and configure the clients as WINS clients. You can configure the WINS server address as part of your DHCP scope, or you can configure it manually.

Accessing Exchange from the Internet

to top

Question:

Hey Dr. Tom,
Is there any other way to access calendar tasks etc., basically use a full functioning Exchange, without using Outlook Web Access? Thanks! – Mark.

Answer:

Yo Mark! You don't care for OWA? I don't blame you. While OWA is nice in a pinch, it's not something I could use for real work, and you're right about the full access to Outlook/Exchange calendaring. But I've got great news for you. Rip out the black box firewall you're using right now and put a smart application layer-aware firewall that knows how to securely manage communications between an external Outlook client and the Exchange Server on the internal network. What firewall can do this? Only one that I know of: ISA Server 2000! You can use ISA Server and create a secure Exchange RPC Publishing Rule and allow your external Outlook clients to have full access to the Exchange Server, just like they do when connected to the internal network. Give it a try, I think you'll like it! If you need full details on the configuration, check out **"ISA Server and Beyond"**.

Security Advisories

Cumulative Patch for Internet Information Service

to top

If you run IIS anywhere in your company, then you need to keep up-to-date on patches. Microsoft has another roll up patch for you. This cumulative patch will bring your IIS installation up to date as of October 30, 2002. This patch applies to IIS versions 4.0, 5.0 and 5.1.

Read more...

Cumulative Update for Outlook Express 6.0 SP1

to top

If you run Outlook Express, or if you have users in your company running Outlook Express, you know how important it is to keep up on OE patches. More than a few problems have been found in OE 6.0, but this update will bring you up to date on the latest fixes. If you haven't installed it yet, head on over to the site and get fixed up now.

Read more...

AntiOnline Employment Opportunity - Spy on Users for Fun and Profit

to top

Many of you might be aware of the AntiOnline Web site. It's a security and hacker-oriented site that has a lot of interesting information and active discussion boards. Guess what? They're hiring! Your new job will be to spy on the members of the AntiOnline.com Web site. As a member of the AntiOnline Research Division you'll be able to spy on your friend, profile their behaviors, and maybe even put them in jail if you're lucky. Apply fast before they give away the job.

Read more...

News Headlines and Resources

NetWare 4 to NetWare 6 CNE Upgrade

to top

Does anybody run a NetWare network anymore? You bet! Those NetWare networks are still out there, and they're upgrading to NetWare 6. You'll want to study up for the upgrading from NetWare 4 to NetWare 6 exam if you're planning on upgrading soon. Cramsession has the study guide you need to ace the exam!

Read more...

It's Official: No Longhorn Server On Tap

to top

Now here's some good news! There were rumors that Microsoft might release a new server product not so long after Windows 2003 is That would have made a whole lot of studying for Admins wanting to support Windows 2000, Windows 2003, and what was code-named "Longhorn". Looks like "Blackcomb" will be the next Microsoft server after Windows 2003.

Read more...

Windows XP Defrag Utility Command Line Reference

to top

Did you know that Windows XP has a command line interface for its defragger? You bet! The command line interface makes it easier for you to fine-tune control over the defragger, and even use it in scripts. If you weren't aware of this feature, check out the article on the available switches.

Read more...

Crypto for VPNs Q and A

to top

What's the difference between SSL, IPSec, and MPPE? What does crypto have to do with VPNs? What about VPN and wireless networking? These are common VPN questions, and VPN guru Lisa Phifer has the answers.

Read more...

101 Things that Mozilla can do that IE Cannot

to top

Looking for a reason to switch browsers? I always thought that Internet Explorer did everything I needed, but this article does give some food for thought. If you're thinking about moving to a new browser, you should read these 101 reasons for switching to Mozilla.

Read more...

How to Become a Microsoft Beta Tester

to top

How do all these people know so much about Microsoft products before the product is released? They're beta testers! Have you ever wanted to be a beta tester, but didn't know how to go about doing it? Check out this Web site and learn how.

Read more...

Safeguard Windows 2000 Terminal Servers from Attack

to top

You need to be careful when you run Terminal Servers on your network. An attacker can use the Terminal Server as an ideal launch point for further attacks if the attacker can take control of your Terminal Server. Check out this article for details on how to protect those Terminal Servers.

Read more...

Download of the Week

FolderMon

to top

Have you ever wanted an easy-to-use tool that would alert you when files were added, removed, and changed in a particular folder on the local hard disk, or on a folder on a network file server? Maybe you want to be alerted for changes made to your Web directories, which are supposed to be read-only? If so, FolderMon is what you need! Changes can be written to a log file, so you have a paper trail of all changes made to files within a folder. Worth checking out!

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.