Windows Insider
37,000 Subscribers Worldwide
May 1, 2002
Issue #90
CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters CramSession

Feature

Building a Split Windows 2000 DNS Infrastructure

to top

Does it seem like more companies and individuals are taking charge of their own Internet services, or am I just traveling in different circles? Seems like everyone wants control over their own Web sites and mail

servers. Maybe it's because the cost of a good high-speed connection is lower than it has ever been before. In our area, we get a 99.99% uptime T1 connection for less than $400US/month. With prices like that, who needs a 3rd-party to mismanage your services when you can do that yourself!

All kidding aside, managing your own services is a rewarding experience. There's nothing like having control over your own servers on your own premises. Sure, if you're running a $100,000,000 company you'll probably want to outsource some of your services so you can make some extra cash by suing the provider if something goes wrong, but if you're a smaller shop, why not just take the bull by the horns and do things yourself? That's what you get paid to do.

If you find yourself in the position, one of the first things you're going to need to take care of is your DNS infrastructure. Are you going to use the same domain name for internal and externally accessible network resources? Are you going to use different names? If you host resources that are accessible from the Internet, you're going to need to configure two DNS zones – one for use on your internal network, and a second that's used by Internet users to get access to your internal network resources. This DNS division of labor is often referred to as a "Split or Split-brain DNS".

By far the easiest configuration is to use different domain names for internal and external network resources. You don't run into problems with internal network clients that need access to servers outside of the internal network. For example, suppose your internal and external network domain name was corp.com. You have a web site hosted by an ISP that goes by the name www.corp.com. Internal network clients trying to access the Web site hosted by the ISP will not be able to get a name resolution for the site because you don't host any servers with the name "www" on your internal network. External network clients will get the Web site hosted by the ISP, since they will receive information from a DNS server that contains records for the publicly accessable www.corp.com. What a mess!

However, using the same domain name for internal and external network resources isn't as bad as it seems. If you host you own servers, there is little problem using the same domain name for internal and external network resources, as long as you don't use the same FQDN for two different servers. For example if you host your own Web Site, www.corp.com can be the same machine for internal and external network users. The only difference would be that external network users will access the server via a public address being used to publish the server, and the internal network users would access the server via its private address.

This assumes that you put your public servers on a private address network segment. It's very common to put public servers on a DMZ segment between your Internet router or firewall and the firewall that protects your internal network. Since you're using Windows 2000 in your network, your best choice for a network firewall is ISA Server 2000, although any vendor's firewall will work.

The public DNS servers are placed on the DMZ segment. These DNS servers contain Host (A), CNAME, and MX records for publicly accessible

servers that are on your DMZ segment. What type of servers would you place on your DMZ segment? Public Web server, SMTP relay servers, public NNTP servers, public FTP servers and maybe even a honey pot. All these servers are accessible via IP addresses on the external interface of the Internet firewall that publishes these DMZ servers. The public DNS server contains records that map to these public addresses on the Internet firewall.

The private DNS servers contain records for internal network hosts only; these records contain only private IP addresses. The private DNS servers support the same domain name as the external DNS servers, but the address records are different on the internal network DNS servers because the internal network clients do not need to "loop back" through the external interface of the Internet firewall. They can be sent directly to the private IP address of the server on the DMZ segment.

The key to the success of this split DNS infrastructure is that private records are not contained on the public DNS, and public records are not contained on the private DNS. Public and private users can use different IP addresses to access the same server on the DMZ segment. With this in mind, you realize that you are not going to be performing any zone transfers between the public and private DNS servers. Although they have zones with the same name, they are not the same zones! Their resource records are completely different.

For security reasons, you may want to use the DNS servers on the DMZ segment as forwarders for the internal network DNS servers. However, if you choose to this option, you have to take some measures to protect your publicly available DNS servers from Internet criminals. The reason for this is that if you choose to allow your public DNS servers to perform recursion for your private network DNS servers, they will also be able to perform recursion for external network users. DNS servers that perform recursion for DNS clients may be open to cache-poisoning attacks.

When the DNS cache is poisoned, attackers can redirect users to a bogus server. An Internet criminal can send a DNS query for a domain (zone) that your DNS server is not authoritative for. If your public DNS server is configured to allow recursion, it will perform a series of iterative queries to resolve the name to an IP address. To poison the cache, your public DNS server queries the authoritative server for the non-local domain, which is "owned" by the Internet criminal. The server will send a valid response AND an attack at the end of the answer to alter the DNS cache.

There are a couple of ways you can protect yourself from DNS cache poisoning attacks:

1. Configure the public Windows 2000 DNS server to "secure the cache against pollution"
2. Create a "split-split" DNS infrastructure

You can go into the Advanced settings of your Windows 2000 DNS server and put a checkmark in the "secure the cache against pollution" checkbox. This effectively prevents the Internet criminal's DNS server from sending extra data in the DNS response to your public DNS server.

The split-split DNS allows one or more of your DMZ DNS servers to perform recursion while the other DNS servers do not. Only the internal

network DNS servers are allowed to use these DNS servers to perform recursion and Internet users never have contact with the DNS server that perform recursion. Any DNS server available to Internet users is not configured to perform recursion. You can disable recursion on a Windows 2000 DNS server by going to the Forwarders tab in the DNS server's Properties dialog box. Place a checkmark in the "do not perform recursion" checkbox.

Setting up DNS servers to support hosting your own Internet services is a fun and challenging endeavor. If you're new to network administration and engineering, you'll learn a lot about how DNS works. If you're an seasoned pro on intranet DNS services, you'll get new insights by deploying a DNS infrastructure that allows Internet hosts to access resources under your total control.

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.
In NT4.0, you can run a VPN (PPTP) RAS server with an incoming address on the same subnet as the "private" network. For example, you might own a Class C subnet of 200.200.200.0, and run a PPTP server on 200.200.200.200. A firewall can block outside access to all but the RAS server, but RAS clients connecting to that server now have access to the entire subnet. On the surface, Windows 2000 doesn't allow this. Is there a sneaky way to do it?
--Mfabuzz

Uncle Bill says:

Yo Mfabuzz! Keep in mind that a VPN is an integral part of your security configuration, so trying to think of ways around it is showing a predilection towards a criminal mentality. We don't want to see you hammering rocks for the next twenty years, so design those VPNs right. Best way to implement your VPN is to put a firewall in front of the Windows 2000 VPN server and configure packet filters in the firewall that will pass the appropriate protocols to the external interface of the VPN server. If this a VPN server only, do not install the RRAS NAT service, and assign a public address to the external interface and a private address to the internal interface. Use those public addresses where they belong: on the DMZ segment only.

Question:

Hi, Uncle Bill
Our DNS generally works fine, it is configured to contact two external "public" DNS machines in order to transmit packets that go externally. Unfortunately, I have had to delete and redo the DNS after we installed an antivirus package, and now a niggly problem has come up. As soon as the external DNS is down, our internal mail is not delivered. [of course

the external ones are not delivered either.] This is the only Win 2000 error that I have come across: Registration of the DNS record '_ldap._tcp.Default-First-Site-Name._sites.domain.com. 600 IN SRV 0 100 389 server.domain.com.' failed with the following error: DNS operation refused
How to fix? please help! [in detail] thanks and take care
--Emma

Uncle Bill says:

Hey Emma! Not exactly sure how you have things configured. I hope you're not using an external DNS server to host your private DNS records! I would first bring all DNS servers hosting your private DNS information back into the internal network fold. There's no reason to let Internet criminals have access to your private network information. SMTP mail delivery depends on MX records. Do you have MX records for your internal mail domain? Mail delivery between internal clients and servers should use the private DNS database, which does not contain any public records. External network users should use a public DNS server that contains MX records that point to the external interface of your firewall, which I assume is publishing your mail servers or mail relay servers.

BTW – the error that you're seeing is probably related to the fact that the downed server dynamically registered some records and the new server is not able to overwrite them because it does not own those records. You can manually delete the old records so the new server can write its own information.

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

to top

E-mail Editor Flaw Could Lead to Script Execution on Reply or Forward

Outlook 2000/XP both let you use Word as your email editor. I used to shun Word as an email editor, but I find it's pretty useful for communicating complex concepts via email. However, there's a vulnerability an attacker could exploit by sending a specially malformed HTML e-mail containing a script to an Outlook user who has Word enabled as the e-mail editor. If the user replied to or forwarded the e-mail, the script would then run, and be capable of taking any action the user could take.

Read more...

News Headlines and Resources

to top

Dealing with PC Power Issues

Do you think the computer's power comes from that fan in the back of

the box? If so, you need to brush up on PC Power issues! Are all power supplies created equal or are some more equal than others? Check out this article by Deb Shinder and find the answers!

Read more...

Windows XP SCSI Drives are Dog Slow

to top

So you paid through the nose for a 15,000 RPM SCSI drive for your new Windows XP computer, and find it has the performance of a 5400 RPM IDE drive? You might need the special SCSI fix for Windows XP from Microsoft.

Read more...

Reg Keys used by the System Restore Utility

to top

The Windows XP System Restore Utility is a great tool that helps you back out of problems created by Malware and other nasty software programs that whack your system. The Wizard makes it look easy; too easy! Check out this article and see how System Restore utility works until the hood.

Read more...

Searching for the Missing Link

to top

What cool service in Windows 2000/XP gets the least fanfare? If you said the distributed link tracking service, we agree! Distributed link tracking fixes problems with broken links and allows you to move your files around without having to recreate shortcuts. Check out this article by Marcin Policht to learn about the details.

Read more...

Use Local Spam Laws to Sue Spammers back to the Stone Age

to top

Did you know that many US States have laws against spam and other Internet crimes? You might just be lucky enough to live in one! For example, if you live in Arkansas, you might be able to get a spammer or script kiddie put away on a felony charge. COOL! Check for your state here.

Read more...

Ten Things to Like about Windows XP Security

to top

Want reasons to give to your boss to upgrade those Windows 2000 Pro or Windows NT 4.0 Workstation machines to Windows XP? How about Security? Roberta Bragg gives you ten strong reasons why you should upgrade to Windows XP.

Read more...

Is .NET Server in Your Future?

to top

The Gartner Group has an opinion about everything. This time it's about whether you should consider upgrading to .NET Server when it's released

sometime in 2003. Bottom line: if you're migrating to Windows 2000 now, keep up the good work and pass on .NET. If you're thinking of upgrading from Windows NT 4.0 sometime next year, you might want to consider .NET Server.

Read more...

9-ISA Server Info Clearing House

to top

If you're not a regular visitor to labmice.net, you're missing out on a lot of cool info! They just put together a great clearing house of information on ISA Server. Makes a nice companion to the www.isaserver.org Web site.

Read more...

Microsoft Windows XP: Internet Connection Firewall

to top

In this session they will discuss using and configuring the Internet Connection Firewall that is included with Windows XP, as well as basic troubleshooting for some common issues you may encounter when using ICF.

Read more...

Download of the Week

Windows XP Power Toys

to top

They're back! The Windows XP Power Toys were axed from the Microsoft web site a couple of months ago for mysterious reasons. Now they're back! Of course, TweakUI is there and there are a bunch of other cools tools too! Microsoft has made it easy to pick and choose what Toy you want. Just download those that look like fun and leave the rest.

Read more...

Free Cramsession IT Newsletters - Choose Your Topics!

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

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

Developers Digest • •

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,
or visit the CramSession Unsubscribe Page .