Net Admin Weekly
59,000 Subscribers Worldwide
February 19, 2003
Issue #27

Feature

Multilayer Network Protection with ISA Server 2000 Part 2: Circuit and Application Layer Filtering

to top

Last week we went over how ISA Server uses packet filter to protect

itself and your internal network from being victimized by Internet criminals. This week we finish off our discussion ISA Server's multilayer protection by examining its circuit and application layer filtering capabilities.

Circuit Filtering

Packet filtering is a widely used and understood concept for many network administrators, but circuit filtering might be less familiar to you. Microsoft's ISA Server documentation makes scant mention of it, and TechNet contains only a few references to it. In fact, circuit filtering seems to be "lumped in" with packet filtering in most discussions, as though the two were the same.

In fact, there is an important difference, but there's nothing mysterious or difficult to understand about it: Circuit filters simply operate at a higher layer of the OSI model, the Transport Layer (the Host-to-Host Layer in the DoD model). Circuit filters restrict access on the basis of host machines (not users) by processing the information found in the TCP and UDP packet headers. This allows you to create filters that would, for example, prohibit anyone using Computer A from using FTP to access files on Computer B.

When circuit filters are used, access control is based on TCP data streams or UDP datagrams. Circuit filters can act based on TCP status flags and sequencing information, in addition to source and destination addresses and port numbers (UDP has to use addresses and port numbers).

Circuit-level filtering applications are often called circuit gateways. Possibly the most famous (or infamous) circuit gateway application is SOCKS, which was originally designed to run on UNIX computers. SOCKS uses sockets to represent and keep track of individual connections. A SOCKS server handles requests from clients inside a firewall and either allows or rejects connection requests, based on the requested Internet destination or user
identification.

The ISA Firewall service works at the circuit level with most Internet applications and protocols, making them perform as though they were directly connected to the Internet. This is true both for clients that have the firewall client software installed and for those that don't (the latter are known as SecureNAT clients). If the firewall client is installed, Internet applications using the Winsock interface send their requests, along with user credentials, directly to the Firewall service.

For SecureNAT clients, it works a little differently. In this case, circuit-level filtering uses a SOCKS filter to forward requests from SOCKS 4.3a applications to the firewall service, or sophisticated "smart" Application Filter that take the place of application specific circuit gateways. The interaction between the SecureNAT client and the firewall service on the ISA Server more closely resembles the traditional circuit gateway.

Circuit-level filtering allows you to inspect *sessions* rather than

packets. A session is sometimes thought of as a connection, but actually a session can be made up of more than one connection. Sessions are established only in response to a user request, which adds to security. This allows computers running a SOCKS client application or the Firewall client to support complex protocols that require secondary connections. Simple protocols that require a single connection do not require circuit filtering because a single session is involved. Complex protocols, such as FTP, SIP and H.323 require multiple sessions that consist of multiple primary and secondary connections. Simple packet filters cannot manage these multisession "circuits", but the talented Firewall (or SOCKS) client and Firewall service have no problems.

Remember that circuit filters don't restrict access based on user information without the help of a client based application such as the Firewall client; they also cannot interpret the "meanings" of the packets. That is, they cannot distinguish between a GET command and a PUT command sent by an application program. To make this distinction, you'll have to use application filtering.

Application Filtering

At times, you might want to filter packets based on the information contained in the Application layer data itself. Packet filters and circuit filters don't use the contents of the data stream in making filtering decisions, but you can do this with application filtering.

An application filter operates at the top layer of the networking model, the Application Layer. Application filters can use the packet header information but are also able to allow or reject packets on the basis of the data contents and the user information.

You can use application filtering to control access based on the identity of the user and/or based on the particular task the user is attempting to perform. With application filters, criteria can be set based on commands issued by the application. This means, for example, that you could restrict a particular user from downloading files to a specified computer, using FTP. You could allow that user to upload files via FTP to that same computer. This is possible because different commands are issued depending on whether the user is retrieving files from the server or depositing them there.

Firewalls using circuit layer filtering and/or application layer filtering are sometimes said to be operating at the "proxy level". You might hear these called circuit or application gateways. An advantage of proxy-level firewall functionality is that these gateways can be configured to require user-based authentication, whereas IP layer firewalls (packet filtering) and simple clientless circuit filtering firewalls, cannot.

Many firewall experts consider application gateways the most secure of the filtering technologies. Their filtering covers a much broader span than the other methods. For example, sometimes hackers write malicious programs that use the port address of an authorized application, such as port 53, which is the Domain Name System (DNS) address. A packet or circuit filter would not be able to recognize that the packet is not a valid DNS request or response and would allow it to pass

through. An application filter, however, is able to examine the contents of the packet and determine that it should not be allowed.

Application filtering sounds like the perfect solution to all your security concerns, but it does have drawbacks. The biggest problem is that there must be a separate application gateway for every Internet service that you need to support. This makes for more configuration work; however, this weakness is also a strength that adds to the security of the firewall. Since a gateway for each service must be explicitly enabled, you won't accidentally allow services that pose a threat to your network.

Application filtering is the most sophisticated level of filtering performed by the firewall service and is especially useful in allowing you to protect your network against specific types of attacks such as malicious SMTP commands or attempts to penetrate your local DNS servers.

Summary

We finished up our lessons on how firewalls filter communications between the internal network and the Internet. You should now have a better understanding of how firewalls carry out packet filtering, circuit filtering and application layer filtering. Next week we'll explore firewall and connection fault tolerance and load balancing. See you then!

This week's feature article by
Deb Shinder MCSE, etc.
Net Admin bi-Weekly Author
Co-Author, Configuring ISA Server 2000
Co-Author, ISA Server and Beyond

Q & A

Question: Denied Access to RRAS Console

to top

Question:

Hi Dr. Tom,

Thought I'd install RAS on my home ISA server and tinker with VPN a bit. Here's where I've hit a wall. I turned on RRAS through ISA using a domain admin account. It started the RRAS service, and opened 256 VPN ports (128 each PPTP and L2TP, which I will reduce asap). So far so good. But, when I open the RAS MMC, my member server's name has that god-forsaken red X beside it. Even worse, when I right-click on it and select properties, I'm told "You do not have sufficient privileges to perform that function". Pardon me!?!?! I even tried it once with my enterprise admin account. Same thing. Whoa! If anyone has come across this or something similar, I'm all ears. Thanks kindly --Mike

Answer:

Hey Mike, we've got some good news for you. This is a common problem. You might have been a little too vigorous in your security of the ISA Server's W2K based operating system. Go back

into the Service Console and find the Remote Registry Service. Turn the Remote Registry Service back on. Close and open the RRAS console again. Voila! No more permissions problems. Another thing to watch out for is Diskeeper and pcAnywhere. You'll find that you won't be able to view the alerts in the ISA Management console when these applications are installed on the ISA Server.

Question: How to Join Two Networks over the Internet

to top

Question:

OK, I'm having trouble getting my head around this one. Maybe someone out there has some suggestions to help me out. I have two Windows 2000 servers that are several thousand miles apart. Both are configured with 192.168.x.x addresses on all of their interfaces. They are connected to the internet through routers. How do I configure one machine to establish a VPN connection to the other when neither machine has a public IP address? Any help here, I'm desperate. --Jay
MCSA, A+, Network+, Linux+

Answer:

Hi Jay! What you want to do is create VPN gateways. The gateways will connect the networks using a VPN. The challenge is to configure your routers so that they establish a gateway to gateway link. This creates a tunnel between the two routers. The next step is to create a VPN tunnel between the two Windows 2000 RRAS servers. You can create this tunnel inside the tunnel between the two routers. The details for creating VPN gateways between Windows 2000 RRAS servers are at http://www.microsoft.com/windows2000/server/evaluation/features/deplyr2rvpn.asp You need to dive into your router documentation to determine how to create the gateway links between the routers.

Security Advisories

Windows XP Passwords Rendered Useless?

to top

There's a big brouhaha over Windows XP and the Windows 2000 Recovery Console. Turns out that if you can boot into Windows XP using a Windows 2000 CD, you can get administrator access to everything using the indows 2000 Recovery console. Not bad! Check out the link for details.

Read more...

Spammers Use Tracking code in HTML Spam

to top

As if the spam wasn't bad enough, now the scumbags are putting tracking information in the stuff to see if you've opened it. If you have, then congrats, you get more spam.

Read more...

Securing ASP.NET Web Services

to top

ASP.NET offers a complex framework that Web app developers can use to provide Web services. The complex something is, the more difficult it is to secure. Check out this article if you're responsible for securing ASP.NET applications on your network.

Read more...

News Headlines and Resources

CCIE Security Exam 350-018 CramSession Now Available

to top

The CCIE continues to be the top of the heap as far as study guides go. Are you getting ready to tackle the 350-018 CCIE Security exam? If so, don't forget to grab the new CramSession for the exam. It'll provide a great cram for the morning of the exam.

Read more...

Active Directory Security Tips and Practices

to top

Getting a good understanding of Active Directory can be rough, but the time you put into learning its inner workings can really pay off. The next step is learning how to secure the Active Directory. Check out this great article by one of Microsoft's format Active Directory experts for some very useful Active Directory security tips and tricks.

Read more...

The FIXPRNSV.EXE Utility

to top

Did you know the Windows 2000 CD includes a command line utility that helps you resolve printer driver issues? Fixprnsv.exe can replace bad drivers with Microsoft printer drivers that work. Very handy little tool.

Read more...

Securing Windows 2000 Server Delivery Guide

to top

Here is "the" guide for rolling out a complex stem to stern security project based on the Microsoft Solutions Framework. This ain't no "how to" security guide; it's a mind bending ride through security project management. It takes a special breed to go through this kind of material without going insane. If you can read through this entire article, then you have what it takes to be a security project manager.

Read more...

Exchange - Technical White Papers (All)

to top

Do you dream of being *the* Exchange guru on your street? If so, then here's your dream come true! A one-stop shop for all Exchange 2000 technical White Papers as of 9/4/2002. It's a single 18 MB download. Be

sure to get this before going on vacation <g>.

Read more...

Sizing and Tuning IIS 5.0

to top

Build it and they will come. But what if too many come? Will your Web server be able to stand up to the strain? Check out this IIS 5.0 Sizing and Tuning White Paper and don't get caught with your pants down.

Read more...

Support WebCast: ISA Server, An Overview of Feature Pack 1

to top

This Support WebCast reviews the new Microsoft Internet Security and Acceleration (ISA) Server Feature Pack 1 features. This includes a discussion of the Link Translator, OWA Wizard, RPC Wizard, SecureID Filter, URLScan for ISA Server, and Delegation of Basic credentials.

Read more...

Download of the Week

3DNA Desktop

to top

Windows XP introduced a new Mac like interface, but it really isn't much different than the desktop interface we first saw with Windows 95. How about really breaking the mold and entering the realm of the true to life 3D interfaces? If you have a powerful video adapter (at least 64 MB memory) and a fast processor, then take your interface to the next level with 3DNA. This interface is extremely cool. You'll feel like you're using one of those computers they have in the movies! Check out the 30 day trial version 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.