Net Admin Weekly

59,000 Subscribers Worldwide

February 06, 2003
Issue #26

CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters

CramSession

Feature

Q & A

Security Advisories

News Headlines & Resources

Download of the Week

Feature

to top

Multilayer Network Protection with ISA Server 2000 Part 1: Packet Filtering

As you probably noticed during our discussion of “stateful” firewalls a few week’s ago, firewall products support the filtering of messages to either allow data to pass through or prevent data from doing so, according to criteria your set on the firewall. At that time I covered general firewall filtering issues. Now its time to focus on a specific firewall implementation, Microsoft ISA Server 2000.

ISA Server, when installed in firewall mode or integrated mode, can perform filtering at the Packet Layer (network layer), the Circuit Layer (transport layer), or the Application Layer. This allows ISA Server to use information at multiple layers of the OSI model to control inbound and outbound access to and from the internal network. In today’s article we’ll go over ISA Server’s packet filtering feature and then in the next issue we’ll talk about circuit and application layer filtering.

Packet Filtering

Packet filtering does most of its work at the Network Layer of the OSI networking model (equivalent to the Internetwork Layer of the DoD model), and deals with IP packets. Packet filters examine the information contained in the IP and transport layer packet headers of a message and then either permit the data to cross the firewall or reject the packet based on that information. When packet filtering is enabled, ISA Server intercepts and evaluates packets before passing them on to a higher level in the firewall or to an application filter.

The information used by the packet filter to make its decision includes the IP address of the source and/or destination computer and the TCP or UDP port number. The port numbers are in the Transport Layer header, so technically, although packet filtering generally operates at the Network Layer, it also processes some higher-layer information. Packet filtering allows the data to proceed to the Transport Layer only if the packet-filtering rules allow it to do so.

Packet filtering lets you block packets that come from a particular Internet host or those that are destined for a particular service on your network (for example, the Web server or the Simple Mail Transfer Protocol, or SMTP, server).

Because ISA Server is designed as a security solution, by default enabling packet filtering causes exclusion of all packets coming into the LAN on the external network interface (the interface connected to the Internet)—unless a packet filter or publishing rule exists that explicitly allows them. In fact, even if packet filtering is not enabled, ISA Server will not permit packets to enter the internal network unless you explicitly configure rules to permit access. But packet filter is required if you want to prevent a compromised firewall from threatening your network.

Types of Packet Filters

ISA Server provides administrators with flexibility in configuring packet filtering behavior. Two types of IP packet filters can be configured:

Allow filters. Specifies the packet types that should be allowed to pass through the firewall (either incoming or outgoing traffic). Other than the packet types you have specified, all packets will be prevented from crossing the firewall. For a service on the ISA Server itself to "listen" (monitor traffic) on a particular port, you need to configure a packet filter to allow traffic on that port (unless the port is opened dynamically by a policy or publishing rule). Publishing Rules allow the ISA Server to listen for services located on the internal network.

Block filters. These allow you to explicitly block specified ports. Block filters are used in conjunction with allow filters to give you more flexibility and granularity of control over exactly what traffic will be permitted through the firewall.

Here is an example of how allow and block filters can be used together. You might need to generally allow traffic on a particular port; for instance, you could configure an allow filter to permit incoming e-mail traffic on port 110, which is the traditional port used by Post Office Protocol (POP) mail services. You could also configure block filters to keep mail from particular host machines, which are known to be sources of e-mail viruses or other unwanted network traffic, from crossing the firewall.

Dynamic packet filtering provides higher security because it opens the necessary port(s) only when required for communication to take place, then closes the port immediately after the communication ends. Dynamic packet filtering allows you to create simple packet filters allowing access and automatically creates and tears down response ports on the ISA Server. This is a much more secure solution than using static packet filters for response ports.

Access and restrictions can often be accomplished by policy or publishing rules. In general, Microsoft recommends that rules be used instead of packet filters, when possible. Allowing access by packet filtering can create a security risk. When you use packet filtering to allow specified traffic to access the ISA server, the port associated with that traffic is opened statically. In other words, it remains open. Access policy and publishing rules must also open the necessary ports to let external traffic in, of course; the difference is that these methods open the ports dynamically, which means that the port does not open until a request arrives.

Note that we're talking about response ports when referring to dynamic packet filtering. A port that accepts traffic for a service must always be open. This is a common concern among neophyte security admins because they're concerned that a "port is open" after running a port scan with a freeware port scanner or after going to www.grc.com. If you want to allow selective traffic to the internal network, the port that allows the inbound traffic must always be open. The response ports can be opened and closed dynamically.

When to Use ISA Server Packet Filters

However, some situations require IP packet filtering in order to provide the needed access. In particular, the following situations will dictate that you must use packet filtering instead of policy and publishing rules:

- If you need to allow access to protocols other than the IP protocols handled by packet filters (TCP and UDP), you have to use packet filtering.
- If you use ISA Server to publish servers that reside within a demilitarized zone (DMZ), which is also referred to as a screened subnet, you have to use packet filters to allow access.
- If there are application programs or services running on the computer on which ISA Server is installed and that must "listen" to the Internet, packet filtering, rather than rules, is the appropriate choice.

Packet filters cannot perform filtering based on anything that is contained in the application layer, nor can it use the state of the multisession communication channel to aid in making its decision to accept or reject the packet. If you need filtering decisions made on the basis of either of these, you need to use filtering that operates at a different layer (circuit or application filtering). Circuit and application layer filtering is what we'll talk about next week.

Summary

ISA Server's packet filtering mechanism is an effective way to control inbound and outbound access to and from ISA Server's external interface. The dynamic packet filtering feature also makes is easy to create a public address trihomed DMZ, because you don't have to create static packet filters to allow response ports to open. Response ports are opened and closed automatically. While packet filters have fairly limited application on an enterprise firewall like ISA Server, they provide the first prong in ISA Server's trident of packet filtering, circuit filtering and application filtering.

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: WINS Server Takes a Dump

to top

Question:

Hi Dr. Tom,

I was given the task of rebuilding our WINS. How should I go about this. I have 5 locations with a WINS server in each location. All remote servers are configured to push - pull with our main site. Thanks in advance. –Pru22

Answer:

There are a number of things you can do to rebuild a WINS database. You could restore from the latest backup of your WINS database; not enough admins back up their WINS database, but they should! If the WINS database isn’t completely destroyed, you can try to increment the WINS server’s highest version number by increasing the “Starting Version Counts” box on the WINS server Properties dialog box. You won’t be able to use that method if the WINS server machine is completely whacked. Since you have a WINS replication network already configured, the best thing you can do is use replication to restore the database. Assuming that your convergence time is low, your WINS server will be up and running with a good database in no time. Two Registry entries control how this works:

Name: InitTimeReplication
Data Type: REG_DWORD
Description: If the value of InitTimeReplication is set to 1, the default value, the WINS server pulls replicas of new database entries from its partners when the system is initialized or when a replication-related parameter changes; if the value is 0, replication occurs only as often as specified by the value set for Replication interval in the Replication Partner Properties dialog box.

Name: InitTimePause
Data Type: REG_DWORD
Description: The value set here determines whether WINS starts in a paused state and remains in that state until its first replication is complete. If the value of InitTimePause is 1, WINS starts in a paused state; if the value is 0, the default value, WINS does not start in a paused state. In the paused state, WINS does not accept any name registrations, releases, or queries. WINS remains in the paused state until it has replicated with its partners or until its first replication attempt has failed. Note that if the value of InitTimePause is set to 1, then InitTimeReplication (in the Pull partners subkey) should be set to 1 or be deleted from the registry

WINS database problems can be a real pain, but if your replication network is up and running and properly configured, the pain will be minimal.

Question: W2K Pro Using the APIPA Address

to top

Question:

I upgraded the CPU on a windows 2000 pro machine, and now cannot get an IP address from our DHCP server (an NT 4.0 domain controller). Instead, I get an Autoconfiguration IP address of 169.254.253.223. I tried ipconfig /renew, I tried to give it a static IP address, but nothing worked. The cable is good, and the light on the switch shows a good connection. Any ideas on how to resolve this? Usually swapping out the NIC will do the job, but not this time. --MysticWeasal

Answer:

Hey Weasal, interesting problem! I’ve seen similar problems with flakey network interface drivers and cheapo NICs. You have to disable and enable the adapter and hope that it works. You say you replaced the NIC, so it doesn't sound like a NIC problem. Does the Event Viewer show any important information? Maybe you have duplicate names or addresses on the network? That would be reported in the Event Viewer. Maybe when you replaced the CPU you harmed some of the motherboard circuitry? I would create a second Windows 2000 Professional installation on the machine and see if you have the same problem. If you do, then you may have some difficult to solve hardware problems. You might even want to put the old processor back in, just to confirm that its not a processor specific problem. However, if it does work with the old processor, you may have a reportable incident. Good luck!

Security Advisories

Flaw in how Outlook 2002 handles V1 Exchange Server Security Certificates could lead to Information Disclosure

to top

A vulnerability in Outlook 2002 exists because there is a flaw in the way Outlook 2002 handles a V1 Exchange Server Security certificate when using the certificate to encrypt email. The flaw prevents Outlook from encrypting the mail correctly. This could cause the information in the e-mail to be exposed when the user believed it to be protected through encryption.

Read more...

Hackers Show Their Colors: Deface NASA Site

to top

Here's one that really takes the cake. Some hacker group called Trippen Smurfs hacked the NASA site on the day of the Columbia tragedy. I takes all kinds to make a world, but we probably could do with fewer of some kinds.

Read more...

Exchange 2000 in the Enterprise: Tips and Tricks Part Two

to top

You Exchange Server is likely the heart and soul of your business. If that baby goes done, no one is going to be happy. That means keeping it secure, especially if its going to be accepting Internet connections. This is a GREAT article by the venerable security expert, Tim Mullens. I guarantee you'll think about something you haven't considered before after reading this
piece.

Read more...

News Headlines and Resources

NAS and SAN: What they Do and How They Differ

to top

Have your storage requirement exceeded what you can do with a traditional file server? You might want to check out NAS and SAN. These storage options are becoming increasingly popular and if you're not sure what they're all about, then check out Deb Shinder nice intro to the subject here.

Read more...

Stop W2K from Assigning WINS/DNS Addresses to RAS Clients

▲ to top

Do you have RAS/VPN clients that have their name resolution settings messed up because the Windows 2000 RRAS Server assigns them WINS and DNS server addresses? If so, you might be interested in how to prevent the RRAS server from automatically assigning RAS/VPN clients name server addresses. This KB article shows you how.

Read more...

Primary and Secondary DNS Server Configuration for ISPs

▲ to top

Are you hosting your own email and Web sites? Do you need to maintain your own DNS records? If so, you should check out this article on how to maintain primary and secondary DNS servers. While aimed at ISPs, it applies to anyone who maintains his own DNS public DNS servers.

Read more...

All About RAID

▲ to top

Quick Quiz: How many types of RAID are there and what are their names? Don't know? Neither did I! Check out this nice rundown on RAID types. Good chance there are a few there you didn't know about.

Read more...

Braindump Owner Sentenced

▲ to top

The infamous braindump seller, Robert Keppel, was sentenced by US District Court last week to 12 months and 1 day in federal prison and ordered to pay Microsoft $500,000 in restitution for his theft of trade secrets. This guy ran the CheetSheets Web sites. Shows that sometimes justice is done.

Read more...

The Unihomed Web Cache Mode ISA Server, Part 2: Web Publishing Outlook Web Access

▲ to top

You want to bring ISA Sever into your organization, but you're not sure about making it your front end firewall. No problem! You can leverage the superior Layer 7 protection provided by ISA Server by publishing your Outlook Web Access sites using a unihomed ISA Server. The article gives you all the details.

Read more...

Support WebCast: Microsoft Internet Information Services (IIS)

▲ to top

6.0, UNC, and Remote Storage

Configuring IIS 6.0 with remote storage content has always been a challenge because of security and scaling issues. IIS 6.0 is the first version of the Web server where remote storage has been optimized to work for high volume and high site density (such as shared hosting) environments. They'll discuss situations where an infrastructure architect would build this type of configuration, the benefits and tradeoffs, and the details of configuring and optimizing IIS 6.0 with remote file servers.

Read more...

Download of the Week

MVsoft PCinfo for Windows

to top

You're overworked, unpaid and badly in need of a vacation. Now your boss says he wants a complete inventory of the software and hardware on each of the 3500 PCs in your organization. Are you going to walk from PC to PC with a clipboard. No way! Check out MVsoft's PCinfo for Windows. This is one nifty utility and gives you complete and details info about whats in and what's on each computer. Download the trial version to get a taste of what this puppy can do. You're gonna like it.

Read more...

Your subscribed e-mail address is:steven.thode@toadworld.net
To unsubscribe, simply click here and hit "send" in your e-mail reader.