Steven Thode

From: CramSession [listboss@list.cramsession.com]
Sent: Friday, May 02, 2003 4:51 PM
To: Steven Thode
Subject: Net Admin Weekly - Issue 31

Net Admin Weekly
59,000 Subscribers Worldwide
May 2, 2003
Issue #31
CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters
CramSession

Feature

Selecting the ISA Server Client Type — Read it

Q & A

Name Resolution Failing on Simple Network — Read it
ICS Addressing Issues — Read it

Security Advisories

Cumulative Patch for Internet Explorer — Read it
Cumulative Patch for Outlook Express — Read it
Flaw In Winsock Proxy Service And ISA Firewall Service Can Cause Denial Of Service — Read it

News Headlines & Resources

How to pass IPSec traffic through ISA Server — Read it
Windows NT (and Windows 2000) File Size and Partition Size Limits — Read it
Optimize NTFS Hard Disk Performance in Windows servers — Read it
Windows Server 2003 E-mail Services — Read it
Technical Overview of Windows Server 2003 Networking and Communications — Read it
RADIUS Protocol Security and Best Practices — Read it
TechNet Webcast: Secure Mobile Access using Wireless and VPN technologies in Windows Server 2003 — Read it

Download of the Week

Vitrite — Read it

Feature

Feature: Selecting the ISA Server Client Type

to top

So you've decided to dump that aging PIX firewall and upgrade to a true layer 7 aware firewall. Good for you! But which one should you use? If you're working in a Microsoft shop, your best choice, hands down, is ISA Server 2000. One of the first planning decisions you need to make before rolling our your ISA Server firewall and VPN server is what ISA Server clients types you want to support. The type of ISA Server client you decide on will be based on what level of authentication and protocol support you require.

Let's go over some of the features of the different ISA Server client types. There are three types of ISA Server clients:

- Firewall clients: these are computers with the Firewall Client software installed and enabled.
- SecureNAT clients: these are computers that are ISA server clients but do not have Firewall Client software installed.
- Web Proxy clients: this term refers to client web applications that are configured to use ISA Server.

By definition, the Firewall client cannot act as a SecureNAT client for TCP and UDP requests because the Firewall client software intercepts all TCP and UDP Winsock requests. On the other hand, both Firewall clients and SecureNAT clients can acts as Web Proxy clients. If the Web Proxy client configuration cannot handle a request for a resource on the Web, the Firewall and or SecureNAT client configuration can step in. The Firewall client is the only client type that requires you to install client software. You must configure the client machine's web browser to make it a Web Proxy client.

Firewall Client

ISA Server's firewall client is equivalent to the Winsock Proxy client in Proxy Server 2.0; it is used for applications such as RealAudio, Windows Media, IRC, Telnet, and any other Internet service that is written to the Winsock Application Programming Interface (API).

The firewall client software can be installed on any 32 bit Windows operating system. This includes the following:

- Windows 95 OSR2
- Windows 98
- Windows Millennium Edition (ME)
- Windows NT 4.0
- Windows 2000

These are the only operating systems that will run the ISA firewall client software. The firewall client is automatically enabled after you install the software, so you don't need to restart the computer.

Installing the firewall client writes a log file on the computer the client was installed on. This file has setup information that includes useful information as to which services were running during installation and what client applications were installed. The log file is helpful in troubleshooting problems you encounter during installation. Note that if you reinstall the firewall client software, the log file will be overwritten.

The firewall client uses a Local Address Table (LAT) that is installed to the hard disk of the client computer (in the Program Files\Microsoft Firewall Client folder). The LAT file is named Msplat.txt. The LAT is used to determine whether a request made by a Winsock application should be sent to the ISA Server or directly to another computer whose IP address is on the LAT. The LAT defines addresses that are "trusted" by the ISA Server. Communications between trusted hosts (LAT hosts) are not screened by the ISA Server. When the Firewall client computer calls another computer on the LAT, the firewall client software is bypassed and the communications are not mediated by the ISA Server.

The primary advantage of the firewall client is that it allows you to apply access policies to authenticated users. Without the Firewall client, you would only be able to apply access policies based on the IP address of the requesting computer (except for those machines configured as Web Proxy clients). Users are authenticated in the background and can have specific rules, such as bandwidth limitations, applied to their user accounts.

This is the best reason for using the firewall client instead of the SecureNAT client. Another compelling reason to use the Firewall client is that you can use a much wider range of protocols. The SecureNAT client is limited to simple, single connection, protocols. Also, those protocols much be listed in the Protocol Definitions node of the ISA Server Management console. The only time the SecureNAT client can use complex protocols is when there is an application filter in place to support that protocol. The FTP Access Application Filter is an example of such a filter.

SecureNAT Client

Any computer configured with a default gateway capable of routing Internet bound requests through the internal interface of the ISA Sever is a SecureNAT client. Although these computers will not be able to benefit from all the access control features of ISA Server has to offer, it does have the advantage of being a "transparent" ISA Server client. SecureNAT clients do not support user level authentication or complex protocols (without an application filter).

SecureNAT clients can ping external addresses (those on the other side of the ISA Server), while computers configured only as Firewall clients cannot. The reason for this is that the Firewall client only supports TCP and UDP based protocols. The SecureNAT client is able to use non-TCP/UDP protocols such as ICMP and GRE.

If your network setup is simple (that is, if there are no routers between the client computers and the ISA Server) you should set the default gateway of the SecureNAT client to be the IP address of your ISA Server machine. The default gateway is the “way out” of the internal network; it is the address to which packets are sent if their destination address is not on the local subnet. Thus, all Internet traffic will go to the ISA Server machine, which will then forward the requests out over the Internet (assuming the packets are not rejected because of ISA’s packet, circuit or application filtering rules).

You can configure the SecureNAT clients’ TCP/IP settings manually or you can use the Dynamic Host Configuration Protocol (DHCP). If you use DHCP, you must select the “Obtain an IP address automatically” checkbox on the TCP/IP Properties sheet.

If your network is larger and more complex and there are routers between the SecureNAT clients and the ISA Server, the default gateway settings on the clients will be configured with the IP address of the router on the local subnet. In this situation the router must be configured to route Internet bound traffic to the ISA Server.

Other TCP/IP settings, such as the DNS server settings, depend on whether the clients will be requesting data from Internet servers only, or will also be requesting data from internal servers. If the former, you can use the IP addresses of DNS servers on the Internet; otherwise, a DNS server on the internal network, configured to resolve both internal and external IP addresses, should be used.

Web Proxy Client

We mentioned earlier that a computer can be a web proxy client at the same time it is a firewall client or a SecureNAT client. The requirements for a web proxy client are:

- The client must have a CERN-compatible web browser installed
- The web browser must be configured to use the ISA server by name or address

A request for web objects sent from a web proxy client will be directed to the web proxy service on the ISA Server. The web proxy service will determine whether the access is allowed, and may retrieve the requested object from cache (if it is there) or cache the object when it is returned from the Internet.

There are two ways to configure the browser to use ISA Server’s Web Proxy service. If the Web Proxy client has the Firewall client software installed, the web browser settings can be configured automatically during the setup of the firewall client.

If the client isn’t automatically configured, you can manually configure the browser settings to use the Web Proxy service. If you’re using Internet
Explorer, this is done via the Tools | Internet Options | Connections setting. You only have to check a checkbox (“Use a proxy server”) in the LAN Settings property sheet, and enter the name of the ISA Server or array and a valid port number (the default for ISA Server is8080).

The SecureNAT client will use the Web Proxy service regardless of whether you have configured the CERN-compliant settings in the browser (because the default HTTP Redirector settings forward requests to the Web Proxy service), so you might wonder if making these settings are unnecessary. I highly recommend that you configure your SecureNAT client’s browsers as Web Proxy clients. This will allow user/group access controls for Site and Content Rules. With user/group access controls for Site and Content rules, you will be able to control what sites users and /or groups can access and what types of files users and/or groups can access via the Web Proxy service.

Summary

You should choose the ISA Server client type that supports the features you want. Do you want user names in your logs? Configure the clients as Firewall and Web Proxy clients. Do you need to support non-TCP/UDP protocols? Configure the clients as SecureNAT clients. Do you need to support complex, multi-connection protocols? Then use the Firewall client. The good news is that a single machine can be configured as all three types of client.

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

Q & A

Name Resolution Failing on Simple Network

to top

Question:

Hi Dr. Tom,

I've a small network that I'm experimenting with. A single domain Controller is here plus a DHCP server (activated and authorized) that is handing out all the addresses and DNS addresses as well as the gateways for the network. All users have connectivity and can ping by address and DNS resolution. A single Router is here as well creating 2 subnets. Pinging across the router (configured with RIP) is possible only with IP, not DNS resolution. Problem: I can't get clients on the other side of the router to recognize the DNS server on the other side of the router, nor can I get clients to join the domain. DNS is configured with Active directory integrated. All addressing in the network has been checked and triple checked for correctness. HELP!! –MrGFP.

Answer:

Good stuff, MrGFP. From what I understand, you have a simple two segment network. You can ping by IP address, but not by DNS host name. The most common reason for this type of problem is that the clients aren't configured with the correct DNS server address. If the clients are configured with the correct DNS server address, then the problem might be that the Host (A) records aren't entered into the zone. Check your DNS zone file to see if the Host records are there. You will have to manually enter Host records if you have not enabled dynamic update for your zone. If the Host records are there, you could have a problem with unqualified names. Are you pinging by FQDN or just the host name? If you're pinging by just the Host name, make sure the client qualifies the unqualified request correctly by configuring a primary domain membership in the Computer Properties dialog box.

ICS Addressing Issues

▲ to top

Question:

Dear Dr. Tom,

In Windows 2000 Professional I know we can share one Internet connection. I have made a dialup connection to the Internet and enabled sharing on it. But it tells me the IP address of the computer will be changed to something like 192.168.xxx.xxx and will no longer be connected to the existing network. I say OK and when in the client browser I give the IP 192.168.xxx.xxx I'm unable to connect. But, when I connect directly from the pc which has the modem, the Internet connection works fine. I am using a network with 199.199.2.xxx What am I doing wrong? Do I have to change the IP address on the client machines also? –Deepak100

Answer:

Hi Deepak, the problem is that when you enable ICS, it changes the IP address on the internal interface of the ICS computer to 192.168.0.1/24. You need to make sure all the other computers on the network are on the same network ID. The easiest way for you to handle this is to make all the network clients DHCP clients. ICS includes a simple DHCP server that will assign your network clients an IP address, default gateway and DNS server that will allow them all to connect to the Internet.

Security Advisories

Cumulative Patch for Internet Explorer

▲ to top

Time to update Internet Explorer. This update brings you up to date as of April 23. Microsoft considers this a critical update, so don't waste time and get it now!

Read more...

Cumulative Patch for Outlook Express

to top

A vulnerability exists in the MHTML URL Handler that allows any file that can be rendered as text to be opened and rendered as a page in Internet Explorer. It would be possible to construct a URL that referred to a text file that was stored on the local computer and have that file render as HTML. If the text file contained script, that script would execute when the file was accessed. This is critical update, so get it ASAP too.

Read more...

Flaw In Winsock Proxy Service And ISA Firewall Service Can Cause Denial Of Service

to top

There is a flaw in the Winsock Proxy service in Microsoft Proxy Server 2.0, and the Microsoft Firewall service in ISA Server 2000, that would allow an attacker on the internal network to send a specially crafted packet that would cause the server to stop responding to internal and external requests. This is a DoS only and does not compromise network security.

Read more...

News Headlines and Resources

How to pass IPSec traffic through ISA Server

to top

A frequently asked question on the ISAServer.org boards is how to pass an IPSec VPN client traffic through ISA Server. It can be done if, and only if, the IPSec implementation supports a feature called NAT Traversal. If you want to know how to make it happen, check out the link.

Read more...

Windows NT (and Windows 2000) File Size and Partition Size Limits

to top

Don’t get caught not knowing at next weekend’s Microsoft Trivial Pursuit game. Check out these charts on the maximum file sizes each file system supports for each version of Windows NT (including NT 5.0).

Read more...

Optimize NTFS Hard Disk Performance in Windows servers

to top

Everyone uses NTFS for its fault tolerance and security advantages. But good medicine sometimes tastes bad and there can be a performance hit when using NTFS. This article covers some things you can do to perk up your NTFS volumes.

Read more...

Windows Server 2003 E-mail Services

▲ to top

One thing we always missed in Windows NT 4.0 and Windows 2000 was a basic POP3 server. Many smaller organizations just need a basic POP3/SMTP server. With Windows Server 2003 they have it! Check out the link for everything you need to know about the new Windows Server 2003 POP3 service.

Read more...

Technical Overview of Windows Server 2003 Networking and Communications

▲ to top

Should you upgrade from Windows NT 4.0 or Windows 2000 to Windows Server 2003? Maybe. One of the most compelling reasons is Windows Server 2003 advanced network capabilities. This paper gives a good overview of what's new and cool.

Read more...

RADIUS Protocol Security and Best Practices

▲ to top

Setting up a Windows 2000/Windows Server 2003 IAS (RADIUS) server is easy and its even easier to configure your VPN server to use RADIUS authentication and accounting. But there is a lot more to RADIUS design that meets the eye. You need to secure those credentials and a lot more! Check out this White Paper for useful and practical details.

Read more...

TechNet Webcast: Secure Mobile Access using Wireless and VPN technologies in Windows Server 2003

▲ to top

Learn about the scenarios and architecture for securing your mobile access over VPN and wireless networks. This Webcast will also cover new technologies in Windows Server 2003 including VPN Wizards, IPSec NAT Traversal, RAS Quarantine, 802.1X, Radius Authentication (IAS), and Network Load Balancing (NLB). See how you can build a secure connected infrastructure using Windows Server 2003.

Read more...

Download of the Week

Vitrite

▲ to top

There are a lot of cool graphics features available in the Mac that we Windows users just can't match. The good news is that Window transparency isn't one of them! You can use Vitrite to get 9 levels of transparency and see through your windows. It probably won't make you more productive, but it's a nice change of pace. At least its free <g>.

Read more...