

RE: ISA 2004 Firewall client

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-05/msg04381.html>

- *From:* v-terliu@xxxxxxxxxxxxxxxxxxxxxxxx (Terence Liu [MSFT])
 - *Date:* Mon, 28 May 2007 08:05:24 GMT
-

Hello Customer,

Thanks for posting here!

According to your description, I understand that you want to get username and hostname showing in the logs and sessions. If I have misunderstood the problem, please don't hesitate to let me know.

Based on my research, I suggest we try the following steps to see if we can resolve this issue:

Part 1: The green arrow only shows up when the client needs to initiate a TCP/UDP connection to the remote host.

Let him try to telnet to a remote host on port 25 for test, will the green arrow appear?

Part 2: When both Internet Explorer proxy servers and the firewall clients are enabled, the network traffic will either go through web session or firewall session.

HTTP, HTTPS, FTP, etc should go through the web proxy session. As long as that Internet Explorer proxy servers are configured normally, these traffics will be rooted to web proxy session.

As to other network traffics (such as POP3, etc), firewall client if enabled, will pass them through the firewall session.

Part 3: I want to explain How the logs and sessions work:

The Weblogging service receives IP address of the source and destination from ISA/RAS of every Internet connection. It saves the IP addresses and time stamp in the WebEvt.log file in "%windows%\temp". When the scheduled report time (by default it's 4:30 AM every day) comes, a reverse DNS look up is done to the source IP address to find the name of the machine. A entry contains the source IP, destination IP, source machine name (if available through reverse DNS look-up) and time of the connection will be added to the MSDE database, then the webevt.log is deleted. If the reverse

RE: ISA 2004 Firewall client

DNS look up is successful, the machine name will show in the log, otherwise the IP address will show. The IP address is always in the database.

You may check if there are PTR records for those IP addresses in the reverse lookup zone. To do so:

1. Click Start, click Run, type "dnsmgmt.msc" and click OK.
2. Expand your server\Reverse Lookup Zones\<your local subnet>.Subnet.

If the IP address list in the Reverse Lookup Zones, the IP address will be resolved to computer name, and it will be listed as computer name instead of IP address in the Server Usage Report. If there is no IP address list in the Reverse Lookup Zones, it can not be resolved to computer name, so it will appear as IP only.

Pointer (PTR) – For mapping a reverse DNS domain name based on the IP address of a computer that points to the forward DNS domain name of that computer.

PTR records are used to support the reverse lookup process, based on zones created and rooted in the in-addr.arpa domain. These records are used to locate a computer by its IP address and resolve this information to the DNS domain name for that computer.

So I suggest you to add PTR records for the unresolved the IP address

PTR Records can be added to a zone in several ways:

1. You can manually create a PTR RR for a static TCP/IP client computer using the DNS, either as a separate procedure or as part of the procedure for creating an A RR.
2. Computers use the DHCP Client service to dynamically register and update their PTR RR in DNS when an IP configuration change occurs.
3. All other DHCP-enabled client computers can have their PTR RRs registered and updated by the DHCP server if they obtain their IP lease from a qualified server. The Windows 2000 and Windows Server 2003 DHCP Server service provides this capability.

The pointer (PTR) resource record is used only in reverse lookup zones to support reverse lookup.

Note: the report may include some network equipment IP address, you no need to add PTR records for them

Part 4: If we can not resolve the issue after we perform the above steps, please kindly help me collect some information for further investigation:

1. Please capture screenshots on the sessions window and send the pictures

RE: ISA 2004 Firewall client

to me at v-terliu@xxxxxxxxxxxxxx

2. Collect the ISA firewall client configuration information

a. Access the following URL to download the fwctool utility:

<http://www.microsoft.com/downloads/details.aspx?familyid=f20f6267-273d-4870-b1e8-799b261b4786&displaylang=en>

More info:

886993 How to configure, to manage, and to troubleshoot the Firewall client in

<http://support.microsoft.com/?id=886993>

b. Install the utility. You may expand the files to c:\fwctool\ folder.

c. Check the firewall client settings through the UI. Manually input the server address and make sure that the firewall client is enabled.

d. Open a command prompt. Input the following commands:

C:

Cd \fwctool

Fwctool pingserver > c:\fwctool\pingserver.txt

Fwctool printconfig > c:\fwctool\printconfig.txt

Fwctool info > c:\fwctool\info.txt

Fwctool printuserconfig > c:\fwctool\printuserconfig.txt

e. Compress the txt files. Send the package to me at v-terliu@xxxxxxxxxxxxxx

3. Please help to gather the ISA Info:

1) Download the file from the following URL:

<http://www.isatools.org/tools/isainfo.zip>

2) Extract all files to a folder on ISA server.

3) Double click Isainfo.js. This will generate 2 files

ISAInfo2004-<computer-name>.log and ISAInfo2004-<computer-name>.xml in the current folder.

4) Please send these files to me at v-terliu@xxxxxxxxxxxxxx

4. Please also help to gather the ISA logs:

1) Schedule a down time.

2) Open ISA 2004 management console.

3) Expand the server node and highlight 'Monitoring'.

4) In the right pane, switch to the 'Logging' tab, make sure the 'Task

'Pane' is showed there.

5) In the 'Task Pane', click 'Configure Firewall Logging' under 'Logging Tasks', and then switch the 'log storage format' from 'MSDE database' (default) to 'File'.

6) Switch to the 'Fields' tab, click 'Select All', and then click OK.

7) In the 'Task Pane', click 'Configure Web Proxy Logging' under 'Logging Tasks', and then switch the 'log storage format' from 'MSDE database' (default) to 'File'.

8) Switch to the 'Fields' tab, click 'Select All', and then click OK.

9) Click 'Apply' to save changes and update the configuration.

10) Temporarily disable the Firewall service. To do that, please click Monitoring | Services tab, and then right click 'Microsoft Firewall' to choose 'Stop'.

11) Clear the current existing W3C logs. To do that, go to the log saving directory and clean any existing .W3C logs. By default, the logs will be saved to 'C:\Program Files\Microsoft ISA Server\ISALogs'. (Some MDF may not be able to deleted, that's normal.) You may backup them first and then delete them.

12) Go back to the ISA 2004 management console, and then Start the stopped 'Microsoft Firewall' service.

13) Reproduce the problem, stop the service, and then gather the resulting W3C files to me for analysis.

14) Please also let me know the IP address of the testing clients so that I can filter the data.

Hope these steps will give you some help.

Thanks and have a nice day!

Best regards,

Terence Liu(MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – www.microsoft.com/security

=====
This newsgroup only focuses on SBS technical issues. If you have issues regarding other Microsoft products, you'd better post in the corresponding newsgroups so that they can be resolved in an efficient and timely manner.

RE: ISA 2004 Firewall client

You can locate the newsgroup here:

<http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>

When opening a new thread via the web interface, we recommend you check the "Notify me of replies" box to receive e-mail notifications when there are any updates in your thread. When responding to posts via your newsreader, please "Reply to Group" so that others may learn and benefit from your issue.

Microsoft engineers can only focus on one issue per thread. Although we provide other information for your reference, we recommend you post different incidents in different threads to keep the thread clean. In doing so, it will ensure your issues are resolved in a timely manner.

For urgent issues, you may want to contact Microsoft CSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

Any input or comments in this thread are highly appreciated.

=====

This posting is provided "AS IS" with no warranties, and confers no rights.

| Thread-Topic: ISA 2004 Firewall client
| thread-index: Acee111e3Q9hzF/TS/qhI3c2Hnd/bA==
| X-WBNR-Posting-Host: 207.46.19.197
| From: =?Utf-8?B?T21haGFEB24=?= <OmahaDon@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
| Subject: ISA 2004 Firewall client
| Date: Fri, 25 May 2007 07:17:02 -0700
| Lines: 16
| Message-ID: <A8854BCB-B442-43F7-9C20-1FF94CE3ED56@xxxxxxxxxxxx>
| MIME-Version: 1.0
| Content-Type: text/plain;
| charset="Utf-8"
| Content-Transfer-Encoding: 7bit
| X-Newsreader: Microsoft CDO for Windows 2000
| Content-Class: urn:content-classes:message
| Importance: normal
| Priority: normal
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.2826
| Newsgroups: microsoft.public.windows.server.sbs
| Path: TK2MSFTNGHUB02.phx.gbl
| Xref: TK2MSFTNGHUB02.phx.gbl microsoft.public.windows.server.sbs:39377
| NNTP-Posting-Host: tk2msftibfm01.phx.gbl 10.40.244.149
| X-Tomcat-NG: microsoft.public.windows.server.sbs

|
| Hi guys,
| I am trying without success to get ISA 2004 firewall client to work in order
| to get username and hostname showing in the logs and sessions.
| The server is running SBS 2003 upgraded to service pack 2 which has had

RE: ISA 2004 Firewall client

RE: ISA 2004 Firewall client

very

| little problems over the last two years. ISA 2004 is running service pack 3.

| The clients are running XP Pro service pack 2 and the latest firewall client.

| The FW client auto detects the ISA server WPAD has been configured on the DHCP server, but once detected there is no green up arrow on the client icon(

| should it be there??).

| When viewing the dashboard it does not show any FW client and in the session

| view it shows Web Proxy and SecureNAT clients and if a user with admin rights

| logs on the session view shows only domainname \username and no hostname

| only the ip address and everyone else who logs in is anonymous

| I have rerun the CEICW which was no help and reinstalled the FW clients.

| Any help would be most welcome

| Thanks

|

.