

Re: Intermittent Firewall 15108 Events on SBS2003/ISA2004

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-12/msg00821.html>

- *From:* v-criminal@xxxxxxxxxxxxxxxxxxxxxxxx ("Crina Li")
 - *Date:* Mon, 05 Dec 2005 02:13:23 GMT
-

Hi Tom,

Thanks for your reply.

I am sorry for the delayed response due to weekend. Please understand that the newsgroups are staffed weekdays by Microsoft Support professionals to answer your systems and applications questions. Your understanding is greatly appreciated!

Thanks for your time and efforts on the issue. I will look forward to hearing from you soon.

Best regards,

Crina Li (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. 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.

Re: Intermittent Firewall 15108 Events on SBS2003/ISA2004

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.

| NNTP-Posting-Date: Fri, 02 Dec 2005 09:35:05 -0600
| Date: Fri, 02 Dec 2005 15:35:03 +0000
| From: Tom Walker <twalker@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
| User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.2) Gecko/20040804 Netscape/7.2 (ax)
| X-Accept-Language: en-us, en
| MIME-Version: 1.0
| Newsgroups: microsoft.public.windows.server.sbs
| Subject: Re: Intermittent Firewall 15108 Events on SBS2003/ISA2004
| References: <rZ-dnZOuzew-URPeRVnysQ@xxxxxxxxxx>
<S6IXrCv9FHA.1236@xxxxxxxxxxxxxxxxxxxxxxxxxx>
| In-Reply-To: <S6IXrCv9FHA.1236@xxxxxxxxxxxxxxxxxxxxxxxxxx>
| Content-Type: text/plain; charset=us-ascii; format=flowed
| Content-Transfer-Encoding: 7bit
| Message-ID: <j9-dnZrW1No09A3eRVnyiQ@xxxxxxxxxx>
| Lines: 195
| NNTP-Posting-Host: 81.179.30.19
| X-Trace:
sv3-iI3x+3zaCNvA6wqwtM9pxuZA2uAAvXxCVH3BxJ1p0t8ZP1URi6FpKM7VIXIEOorwG/331g
Fss2uGX!mva1uoavAO5d9gQ2y61bdqytbLZ6OeFfQz1WKBQshwvx0i9FRxjcEz3gHf+gqy9PNHIV
7GLWFG5d!mkPhLqK6+nw=
| X-Complaints-To: abuse@xxxxxxxxxxxxxxxx
| X-DMCA-Complaints-To: abuse@xxxxxxxxxxxxxxxx
| X-Abuse-and-DMCA-Info: Please be sure to forward a copy of ALL headers
| X-Abuse-and-DMCA-Info: Otherwise we will be unable to process your
complaint properly
| X-Postfilter: 1.3.32
| Path:
TK2MSFTNGXA02.phx.gbl!TK2MSFTNGP08.phx.gbl!newsfeed00.sul.t-online.de!t-onli
ne.de!border2.nntp.dca.giganews.com!border1.nntp.dca.giganews.com!nntp.gigan
ews.com!local01.nntp.dca.giganews.com!nntp.pipex.net!news.pipex.net.POSTED!n
ot-for-mail
| Xref: TK2MSFTNGXA02.phx.gbl microsoft.public.windows.server.sbs:227308
| X-Tomcat-NG: microsoft.public.windows.server.sbs
|
| Crina
|
| Thanks for the step-by-step guide.
|
| Everything in my setup was as you listed except that I had my server's
| internal IP address in the WINS setting for the external NIC - NetBios

Re: Intermittent Firewall 15108 Events on SBS2003/ISA2004

| was already disabled.

|
| Unfortunately, it made no difference and I still get the 15108 warnings
| – and they specify the IP Address allocated to the PPP Adapter on the
| remote client.

|
| I'm going to try setting fixed IP addresses for the laptops and remote
| clients to see if that stops them.

|
| I'll re-post here when I find out what happens.

|
| Tom Walker

|
| Crina Li wrote:

|> Hi Tom,

|>

|> Thank you for posting in SBS newsgroup.

|>

|> From your problem description, I understand this issue to be: you get
the

|> Warning event 15108 on your SBS 2k3 machine with ISA 2004. If I have
|> misunderstood your concerns, please do not hesitate to let me know.

|>

|> Basically, the ISA server identifies the spoof attacking according to
the

|> routing table and the LAT (for ISA 2004 server, it's the address range
of

|> the internal network object). If the ISA server receives a package with
an

|> internal IP as source address from the external port, the package would
be

|> treated as a spoof attack. For a normal ISA server, the event just
reports

|> the blocked intrusions.

|>

|> Based on my research, it is NORMAL for a 15108 event to be logged if
the

|> network setup is such that the VPN client obtains a network address
from

|> the internal DHCP pool. You can try reserving a static pool of
addresses

|> for VPN users. This static range was then EXCLUDED from the DHCP pool.

|> Once that was done, a VPN client was given one of the static pool
addresses

|> when he connected, and the ISA server no longer detected external
traffic

|> from an internal address because that internal address was in the
excluded

|> DHCP range.

|>

|> More information:

|>
|> This behavior may also occur if both of the following conditions are true:
|>
|> – The internal network adapter on the ISA Server computer points to a
|> default gateway address that is on the internal network.
|> – The network adapter on the server that has the published resource points
|> to the same internal default gateway address as the ISA Server computer.
|>
|> To resolve this behavior, please perform the following steps:
|>
|> 1. Double check if you have removed the default gateway address on the
|> internal network adapter of the ISA Server computer. For ISA Server to
|> function correctly, the internal network adapter should not have a default
|> gateway specified.
|>
|> 1) Click "Start", point to "Settings", and then click "Network and
|> Dial-up
|> Connections".
|> 2) Right-click the internal adapter, and then click "Properties".
|> 3) Click "Internet Protocol (TCP/IP)", and then click "Properties".
|> 4) Remove the default gateway address in the "Default gateway" box, and
|> then click "OK" two times.
|>
|> 2. If there are other internal networks that send and receive traffic
|> through the ISA Server computer, use the route add command with the -p
|> switch to add a persistent static route to each internal network. When you
|> specify the gateway address, point to the internal router that permits
|> access to the other internal networks. Configure persistent static
|> routes
|> on the internal adapter of the ISA Server computer and on the server
|> that
|> has the published resource. For more information about how to use the
|> route
|> command, type route /? at a command prompt.
|>
|> 3. On the server that has the published resource, configure the default
|> gateway address to point to the internal address of the ISA Server
|> computer.
|>
|> 1) Click "Start", point to "Settings", and then click "Network and
|> Dial-up
|> Connections".
|> 2) Right-click the internal adapter, and then click "Properties".
|> 3) Click "Internet Protocol (TCP/IP)", and then click "Properties".
|> 4) In the "Default gateway" box, type the internal address of the ISA
|> Server computer, and then click "OK" two times.
|>

Re: Intermittent Firewall 15108 Events on SBS2003/ISA2004

- |> 4. Please rerun the CEICW again to configure ISA as default settings.
- |> Please refer to the following KB article:
- |>
- |> 825763 How to configure Internet access in Windows Small Business Server
- |> 2003
- |> <http://support.microsoft.com/?id=825763>
- |>
- |> For more info, please refer to:
- |>
- |> 888042 ISA Server 2004 does not support traffic redirection
- |> <http://support.microsoft.com/?id=888042>
- |>
- |> 884496 Client computers cannot access external resources, and event ID 14147
- |> <http://support.microsoft.com/?id=884496>
- |>
- |> 840681 Attempts to access published resources are logged as spoof attacks
- |> with
- |> <http://support.microsoft.com/?id=840681>
- |>
- |> Besides, please check the following:
- |>
- |> 1. Check to see if a WINS server is listed on the WINS tab of TCP/IP properties for existing External network adapters. If there is remove it.
- |> 2. Please disable NetBIOS over TCP/IP on the External adapter from External Connection Properties\TCP/IP properties\Advanced\Wins tab.
- |> 3. Updated the NIC drivers.
- |>
- |> Please do not hesitate to let me know if you have any questions or if you need further assistance.
- |>
- |> Thanks for your time and I look forward to your reply.
- |>
- |> Best regards,
- |>
- |> Crina Li (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

Re: Intermittent Firewall 15108 Events on SBS2003/ISA2004

manner.

|> 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.

|> -----

|> | NNTP-Posting-Date: Thu, 01 Dec 2005 04:12:51 -0600

|> | Date: Thu, 01 Dec 2005 10:12:50 +0000

|> | From: Tom Walker <twalker@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

|> | User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.2)

|> | Gecko/20040804 Netscape/7.2 (ax)

|> | X-Accept-Language: en-us, en

|> | MIME-Version: 1.0

|> | Newsgroups: microsoft.public.windows.server.sbs

|> | Subject: Intermittent Firewall 15108 Events on SBS2003/ISA2004

|> |

|> | I'm getting a small number of 15108 events around the times when a remote user connects through VPN.

|> |

|> | Our internal LAN IP addresses are 10.0.0.x.

|> |

|> | Most of the 15108s quote IP addresses in the 10.0.0.11 to 10.0.0.17

|> | range - all allocated to the server, according to DHCP.

|> |

|> | The other 15108 quotes 192.168.2.2 which I believe is the remote

|> | client's IP address connecting to the remote ADSL Modem/Router

(client

|> | connects via a VPN dial-up).
|> |
|> | Not experiencing any abnormal behaviour connecting or working
remotely
|> | so should I be doing anything about these messages?
|> |
|> | And why does Firewall flag up 15108s for addresses allocated to the
|> server?
|> |
|> | Further info:
|> |
|> | 1. Internal address range in ISA is 10.0.0.0 to 10.0.0.255 plus
|> | 10.255.255.255. DHCP address pool has 10.0.0.1 to 10.0.0.254 with
|> | 10.0.0.1 to 10.0.0.9 excluded (and 10.0.0.113 which is reserved for a
|> | network printer).
|> | 2. Internal server IP (10.0.0.2) has no default gateway and only DNS
|> | entry is 10.0.0.2.
|> | 3. External server IP is 192.168.0.2 with default gateway 192.168.0.1
|> | (ADSL Router). DNS is set to 10.0.0.2.
|> | 4. DNS has forwarders pointing to our ISP's primary and secondary DNS
|> servers.
|> |
|> |
|

• **Follow-Ups:**

- ◆ **Re: Intermittent Firewall 15108 Events on SBS2003/ISA2004**
◇ From: Tom Walker

• **References:**

- ◆ **Intermittent Firewall 15108 Events on SBS2003/ISA2004**
◇ From: Tom Walker
- ◆ **RE: Intermittent Firewall 15108 Events on SBS2003/ISA2004**
◇ From: "Crina Li"
- ◆ **Re: Intermittent Firewall 15108 Events on SBS2003/ISA2004**
◇ From: Tom Walker

- Prev by Date: **RE: Users and Groups**
- Next by Date: **Re: access with run from share but not from DFS**
- Previous by thread: **Re: Intermittent Firewall 15108 Events on SBS2003/ISA2004**
- Next by thread: **Re: Intermittent Firewall 15108 Events on SBS2003/ISA2004**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**