

## Re: Eventid 15108... spoof address ????

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-12/msg02087.html>

---

- *From:* [v-criminal@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:v-criminal@xxxxxxxxxxxxxxxxxxxxxxxx) ("Crina Li")
  - *Date:* Fri, 09 Dec 2005 11:33:31 GMT
- 

Hi Maxibo,

Thanks for your reply.

As I said, the event just reports the blocked intrusions. Also you can monitor how the IP 169.254.142.51 is generated through DNS debug log.

You can collect the following information for analysis:

1. Get the ipconfig/all result on SBS and a client computer.
2. Collect the ISA info:

1) Download the file from the following URL:

<http://www.isatools.org/isainfo/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.

3. 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.

Re: Eventid 15108... spoof address ????

- 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 (initiate an SQL access), stop the service, and then gather the resulting W3C files to me for analysis.

I am appreciated your time and I look forward to hearing from you.

Best regards,

Crina Li (MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – [www.microsoft.com/security](http://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.

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.

-----  
| From: "Maxibo" <totallyanon@xxxxxxxx>

Re: Eventid 15108... spoof address ????

Re: Eventid 15108... spoof address ????

| References: <uBNKst4#FHA.2264@xxxxxxxxxxxxxxxxxxxxxx>  
<J2HRBW6#FHA.3764@xxxxxxxxxxxxxxxxxxxxxx>

| Subject: Re: Eventid 15108... spoof address ????

| Date: Fri, 9 Dec 2005 09:26:41 -0000

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

| |

| Hi Crina

|

| This spoof address is appearing every minute in the event log and damn if

I

| can find it. Site has recently had SBS SP1 installed.

|

| LAT table has the 192.168.16.2 range.

|

| The 169 address I understand as a pc not obtaining an IP address from a  
| source i.e DHCP. All pcs are on the network and have a correct IP

|

| I have also seen active sync 4 generating this 169 address, no palmtops  
| connected on site.

|

| I am still learning ISA 2004, ISA 2000 I could go straight to the  
| firewall

| logs, where are they in 2004?...lol

|

| I can view the ' sessions ' in ISA monitoring and this IP doesn't appear  
| at

| any time.

|

| 169 address is not public so unsure if it is a pc externally? No pcs  
| connect

| remotely (except me) Was wondering if it was something to do with RAS but  
| then the IP appears when I am not connected.

|

| I did find it listed in DNS as an A record and everytime I delete it it  
| comes back.

|

|

|

| ""Crina Li"" <v-crinal@xxxxxxxxxxxxxxxxxxxxxx> wrote in message  
| [news:J2HRBW6%23FHA.3764@xxxxxxxxxxxxxxxxxxxxxx](mailto:news:J2HRBW6%23FHA.3764@xxxxxxxxxxxxxxxxxxxxxx)

| > Hi Maxibo,

| >

| > 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

Re: Eventid 15108... spoof address ????

Re: Eventid 15108... spoof address ????

|> routing table and the LAT (for ISA 2004 server, it's the address range of  
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.  
|>  
|> Please open the ISA management console, navigate to  
|> Configuration->Networks, on the middle pane, double click the Internal  
|> object, go to the Addresses tab, is the correct address range listed?  
|> Please delete any irrelevant entries. Then click Apply to save the  
|> settings.  
|>  
|> Also, can you tell me if the IP address recorded in the event log is  
one  
|> of  
|> the IP address of the internal client?  
|>  
|> Since the SBS server is connecting to the internet, it's expected that  
the  
|> server could receive some spoof attacks from the internet. The ISA  
server  
|> is a firewall product. The potential attacking packages would be  
blocked  
|> by  
|> the ISA server. With the alert function enabled, the attacking  
activities  
|> are logged in the event log. You may also see the blocked packages  
through  
|> the firewall log.  
|>  
|> In most cases, the 15108 spoof attack event is normal for an ISA  
computer.  
|> If you receive many alerts from a consistent public IP address, you may  
|> need to contact the ISP and let them block the particular host. You may  
|> also report the attacker's address to your local security or legal  
agent.  
|>  
|> 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:

Re: Eventid 15108... spoof address ????

Re: Eventid 15108... spoof address ????

|>  
|> 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.  
|>  
|> 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>

Re: Eventid 15108... spoof address ????

Re: Eventid 15108... spoof address ????

|>  
|> 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.  
|>  
|> I am appreciated your time and look forward to your reply.  
|>  
|> Best regards,  
|>  
|> Crina Li (MSFT)  
|>  
|> Microsoft CSS Online Newsgroup Support  
|>  
|> Get Secure! – [www.microsoft.com/security](http://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.

Re: Eventid 15108... spoof address ????



Re: Eventid 15108... spoof address ????

◇ *From:* Maxibo

- Prev by Date: ***RE: RWW not working on some client desktops***
- Next by Date: ***Re: connect to server– instant webslowdown***
- Previous by thread: ***Re: Eventid 15108... spoof address ????***
- Next by thread: ***Re: Eventid 15108... spoof address ????***
- Index(es):
  - ◆ ***Date***
  - ◆ ***Thread***