

## Re: Firewall Client Extremely Chatty

---

*Source:* <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2007-01/msg00181.html>

---

- *From:* "Asher\_N" <[ashernat@xxxxxxxxx](mailto:ashernat@xxxxxxxxx)>
  - *Date:* Tue, 16 Jan 2007 08:09:41 -0800
- 

"Will" <[westes-usc@xxxxxxxxxxxxxxxxx](mailto:westes-usc@xxxxxxxxxxxxxxxxx)> wrote in  
[news:K4edncW4rqKh3zHYnZ2dnUVZ\\_sWdnZ2d@xxxxxxxxxxxxxxxxx](mailto:news:K4edncW4rqKh3zHYnZ2dnUVZ_sWdnZ2d@xxxxxxxxxxxxxxxxx):

"Phillip Windell" <[@.](mailto:@.)> wrote in message  
[news:uU1#luPOHHA.5064@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uU1#luPOHHA.5064@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

How do you think applications like Sysinternals  
TCPView are able to show you connections?

It runs on the Machine that the Executable causing the connection  
runs on,...it is not a network sniffer,...it runs at a much "higher"  
level in

the

system. So if something like TCPView ran on ISA it would only show  
executables that live on the ISA that initiated connection.

But with that said ISA does get similar information from Firewall  
Clients because the Firewall Client has this information (because it  
runs on the client) and passes it to the ISA. I do not think you  
will get all the information that TCPView gives you but it is fairly  
close.

In the ISA MMC,

1. Choose the Monitoring Node
2. Chose the Sessions Tab
3. Right-Click on the Column Headers and uncheck everything except:  
Activation, Client IP, Client Host Name, Application Name
4. Select to Edit the Filter and choose:  
Filter by: "Session Type"  
Condition: "Equals"  
Value: "Firewall Client"
5. Then run the Query.

I did look at sessions, but the "Target" shows as the firewall, not as

## Re: Firewall Client Extremely Chatty

the actual endpoint.

I hate to say this, but isn't this ISA 2004 Firewall Client feature actually a hacker's best friend? I no longer have any idea at all what traffic is leaving my network. ISA hides this from me almost completely. Even exercising the ISA Monitor at the level of individual TCP Open Connection and Close Connection, the target for the firewall client was showing as the firewall, not as the actual target system on the Internet. I would have to go out to my external firewall to see the real target, but because the traffic has been NAT'd at that point, I would have no idea which user is actually generating the request.

Then get something like SurfControl or Websense. The reporting will give you what you need.

ISA's primary function is to protect the network perimeter. It does that very well. The underlying assumption is that it will stop a user from using a protocol they are not authorized to and allow them those that they have access to. What the actual traffic is at that point is none of ISA's concern. If you are allowed to use HTTP, ISA really does not care what sites you go to.

If you don't mind my asking, why are you so paranoid about your outbound traffic?

.