

Re: Best practice – or Microsofts stand on AV engine on ISA servers?

Re: Best practice – or Microsofts stand on AV engine on ISA servers?

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2007-11/msg00141.html>

- *From:* "MS News" <n/a>
 - *Date:* Wed, 28 Nov 2007 13:04:41 -0500
-

As you noted it's not a perfect world, especially when Microsoft produces products like SBS that violate all of the principles about having a firewall be nothing but a firewall. (Tom's article does not mention SBS.)

You can run a file system anti-virus very effectively on your ISA server. You will need to set scan exclusions for the folders where the log files are stored or where the MSDE database is stored. You also will need to exclude the cache file or folder from scanning.

It all comes down to what you will say or do when a network-aware virus trashes your ISA server or someone does use a browser and clicks on something they shouldn't. I am not comfortable with taking that risk myself.

Ray

"Bendji" <Bendji@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:2A25ED25-8983-4F0E-AA39-D274B8E97D67@xxxxxxxxxxxxxxxxxxxx

Greetings all,

I got a question about running an Antivirus (AV Engine) on ISA 2004 or 2006.

Some of the companies I work for have a security police witch states that there should be installed an AV engine (and running) on every client and server in the enterprise. The ISA firewall is also counted as a server and should hence have an AV engine installed.

I've searched the Internet to find a response to: How an AV engine should be configured on an ISA server, but have not found any thing you.

The only thing I have found so far is a post on Thomas Shinders blogs:

<http://blogs.isaserver.org/shinder/2006/05/05/should-you-install-anti-virus-software-on-your-isa-firewall/>

And I can understand Thomas statement in this post, but when I think about it, a lot of people who is administrators of servers log in with RDP. Some even have a setting where they map a drive from the local client. In the blog

Re: Best practice – or Microsofts stand on AV engine on ISA servers?

those people would not be "responsible" administrators :-> (The world is not perfect).

So I kept searching for Microsoft's official stand on the topic and the closest I found was this page
<http://www.microsoft.com/isaserver/partners/contentsecurity.msp>
Witch is about Antivirus filters for http and ftp only and not for the host.

Any one who knows what Microsoft says about running an AV engine on the ISA server and whats best practice for configuration is?

Thanks in advance,

Yours Sincerely,
Benjamin