

Re: Best Practice for Using MVPS HOSTS File on ISA Server?

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2008-04/msg00137.html>

- *From:* "Will" <westes-usc@xxxxxxxxxxxxxxxx>
 - *Date:* Thu, 17 Apr 2008 17:31:12 -0700
-

"Jim Harrison (ISA SE)" <jmharr@xxxxxxxxxxxxxxxx> wrote in message news:EF447E2E-646C-4321-9C6F-5E2F059797F0@xxxxxxxxxxxxxxxx

CIL...

--

Jim Harrison (ISA SE)

This posting implies no warranty and confers no rights.
<http://catb.org/~esr/faqs/smart-questions.html>

"Will" <westes-usc@xxxxxxxxxxxxxxxx> wrote in message news:mIidnevdc9gZJ7VnZ2dnUVZ_ournZ2d@xxxxxxxxxxxxxxxx
"Jim Harrison (ISA SE)" <jmharr@xxxxxxxxxxxxxxxx> wrote in message news:30BF0330-ECE4-492B-B04F-507B4B2BC3BA@xxxxxxxxxxxxxxxx

The rules aren't "compiled".

When you make changes to firewall rules and "Apply" them, you get a modal dialog that announces the changes are being "applied". A compiler is a program that converts text written in one language to some target form. Surely ISA doesn't store the firewall rules in a human-readable form. So in the broadest sense the human readable version of the firewall rules must be getting converted to *some* other form. That meets my test for what compilation mean. It would be good to know what the more formal terms ISA uses for the source and "applied" versions of firewall rules, but I think we are just saying the same things using different words.

[Jim] – No, we're not. While it's possible to apply any verb that meets one's interpretation of events, that ability isn't self-justifying. The point is; the rules aren't "changed" as would be performed by some form of "compilation". What happens is this:

Re: Best Practice for Using MVPS HOSTS File on ISA Server?

1. the current changes are evaluated to determine if the resulting policy is actionable
2. if #1 is satisfied, the rules are "mixed" to produce a list that is ordered according to the context (Enterprise pre-array, array, Enterprise post-array) in a single rule set
3. if #2 is satisfied, the changes are evaluated to determine if they negatively impact ISA functionality (communication with CSS, for instance) if they break ISA, they cannot be applied.
4. if #3 is satisfied, the rules are written to storage
..at this point, you get the "all is good" dialog.

There are human readable forms of the firewall rules, and there is some binary representation that can be acted on by ISA. How you get from human readable to the computer readable form would I think meet any reasonable definition for the word 'compilation'. What you describe is mostly optimization, which is further evidence that what the human reads and what the computer acts on are two different forms of the same information.

In any case, agreement on the meaning of that word is probably not important to this thread. I get your points. :)

The reason I discourage the use of hosts file games is that they quickly become unwieldy and completely circumvent ISA policy structure.

I guess one could assign groups of host names that are the same type of target site in the hosts file to a unique IP that is an internal web server.

As long as you had as many unique target web server IPs as you do types of sites, you should be able to create ISA rules to align to those IP targets.

So one could by some design and discipline at least create some cooperation between the hosts file usage and the ISA rules.

I do understand your point on the hosts file being a very cumbersome vehicle for long term maintenance of many such hosts.

[Jim] – even your alternative is stuck in the hosts file. While my main point for hosts file usage is with maintenance, the biggest issue is in waiting for the inevitable TCP timeout this technique imposes on each and every connection that's made. IOW, it's a literal waste of time.

Yes, but you can have that IP point to a web server that returns a

Re: Best Practice for Using MVPS HOSTS File on ISA Server?

simple image. That image is in turn cached by ISA's proxy. So as long as you don't have timeouts (which as you say would be the default case using HOSTS, and yes it does make the page SLOW) then returning that cached image should be enormously fast.

—
Will

.