

Re: UDP Rule Ignored

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2006-08/msg00029.html>

- *From:* "Will" <westes-usc@xxxxxxxxxxxxxxxx>
 - *Date:* Mon, 31 Jul 2006 23:19:42 -0700
-

Okay, I have a partial solution to this mystery, followed up with an even worse behavior that I think must be a bug.

The reason ISA Server 2004 will show a packet in the monitor but not apply a rule, is when it has no network rule. In this case, it lacked a routing rule back into the one segment with the NTP server. Every other internal network going out is by NAT.

Now, the worse behavior: having introduced an ISA Server 2004 Network rule to route back traffic from the no man's land in to the NTP segment behind the firewall, the traffic flies in and out of the firewall, but the monitor doesn't see the packets at all!!

That has to be a bug?

--
Will

"Will" <westes-usc@xxxxxxxxxxxxxxxx> wrote in message
news:sZKdnZMXiPtZTFPZnZ2dnUVZ_r6dnZ2d@xxxxxxxxxxxxxxxx

I have an ISA Server 2004 rule that seems to be not taking, and what is stranger is how the monitor is showing the packets.

One of our "internal" segments is a dedicated NTP server on Windows that
is

pretty much isolated on its segment and can only get out and in by NTP and

a

proprietary superset of NTP that the vendor supports for the product.

The

box had to be put behind ISA Server 2004 since it is our clock for all the internal domain controllers. I have several boxes in front of the ISA

Re: UDP Rule Ignored

Server 2004, in a no man's land that is behind yet another firewall, that

I

want the same NTP server to service. I could have published the UDP protocol on the NTP server on the ISA, but I decided to flex ISA's capabilities and just route the dedicated internal NTP network out to the

no

man's land, and then I have a route on the no man's land to point back to the NTP server on the dedicated internal NTP network using ISA Server 2004 as the "router".

What I see on the monitor of ISA Server 2004 baffles me. The route on

the

no man's land is working fine. The proprietary NTP UDP variant packets come in with a target IP pointing to the NTP server, presented on the correct interface of the ISA Server 2004. But in the monitor ISA Server 2004 rejects the packets, and the baffling part is that it SHOWS NO RULE

AS

MATCHING. I would expect if I had the rule wrong that the default rule would catch this packet and it would be rejected using that rule.

Instead,

the packet is denied, and NO rule shows as matching on the Denied line of monitor. What the heck would cause that behavior?!

--

Will

.