

Direction paradigm? n00b question

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2007-01/msg00183.html>

- *From:* "AnonymousDog" <andyk@xxxxxxxxx>
 - *Date:* 16 Jan 2007 12:12:20 -0800
-

I'm pretty new to ISA2k4 and am thoroughly confused by the new(er) policy interface and conceptual structure. First, the difference between "system policy" and the other rules is lost on me (particularly since it seems impossible to actually ADD a rule to system policy), but that's not my really my question.

In ISA 2k, packet filter rules made sense to me. They were based on a very simple filter definition that specified IP protocol type, local and remote port numbers (with options for dynamic or all port numbers) and the direction of initial traffic *relative to the ISA server*. There were tabs to specify the identities of local and remote computers. It was conceptually no different from configuring iptables or many "black box" firewalls (e.g., Firebox).

In ISA 2k4, there are no more packet filters...da*n shame, because MS took a conceptually simple task and made it much more confusing. First, it seems that the "incoming" and "outgoing" direction concepts have changed in their point of perspective: Incoming and outgoing used to be relative to the ISA machine itself. Now I can't tell what the point of reference is, but, viewing some of the default system policy rules, it doesn't seem to be ISA.

So here's the questions:

What is the reference point (e.g., ISA machine, LAN, other) from which to determine "incoming" vs. "outgoing" protocols?

That also begs the question about how to duplicate the functionality of ISA 2k packet filters in ISA 2k4. If one is trying to open a port for traffic incoming to the ISA (from local LAN or external nets), is the rule supposed to be a server publishing rule or an access rule (or do you need one of each to cover the "from external" and "from LAN" scenarios). Also, as a packet filter, how do you lock down client ports on an access or server publishing rule? I see no way to do that.

Pls. excuse the minor rant and n00b-oriented questions; I'm a bit turned about on this.

.