

Re: [fw-wiz] Questions about converting FW-1 ruleset to PIX – sor t of...

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-01/msg00082.html>

- *From:* nick leachman <nleachman@xxxxxxxx>
 - *Date:* Tue, 24 Jan 2006 09:10:34 -0500
-

On 1/24/06, Ralf.Zessin@xxxxxxxx <Ralf.Zessin@xxxxxxxx> wrote:

> Hi Nick,
>
>> One of the checkpoint rules denies traffic from all internal networks
>> for a group of specific ports destined to a group that contains all of
>> the DMZ servers and also to the DMZ network itself – a DMZ object
>> group.
>>
>> My questions is: What is the purpose of having the the servers "and"
>> the dmz network listed in the destination? Is this necessary?
>>
>
> No, the information is redundant. But if there is above a rule which
> explizit allows traffic which is blocked by this rule, this traffic
> has to go through.
>
> Checkpoint evaluates its rule form top to down and first (not best)
> match is taken.
>
> But what is this for a rule–design where Ports/traffic are explicit denied
> if it
> was not an alert–rule ? Normaly all traffic has to be forbidden and
> I have to *allow* traffic by rules.
>
> – Ralf
>

Thanks for the feedback Ralf – I'm glad to hear that I was understanding the checkpoint rules correctly.

For the sake of trying to explain this checkpoint rule I over-simplified it somewhat. It actually states "permit traffic sourced from all internal networks to pass outbound (using the list of ports) to anywhere EXCEPT the DMZ".

I guess this is a nice feature of the checkpoint to have a single rule with this level of complexity; but I'd rather (we are creatures of habit, after all :-)) break it up into separate permit and deny rules.

Re: [fw-wiz] Questions about converting FW-1 ruleset to PIX – sor t of...

Thanks again,
Nick

--

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxx
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

• **References:**

- ◆ **[RE: \[fw-wiz\] Questions about converting FW-1 ruleset to PIX – sor t of...](#)**
 ◇ From: Ralf . Zessin

- Prev by Date: **[RE: \[fw-wiz\] False results to DMZ](#)**
- Next by Date: **[Re: \[fw-wiz\] RE: IDS \(was: FW appliance comparison\)](#)**
- Previous by thread: **[RE: \[fw-wiz\] Questions about converting FW-1 ruleset to PIX – sor t of...](#)**
- Next by thread: **[\[fw-wiz\] Gmail replies](#)**
- Index(es):
 - ◆ **[Date](#)**
 - ◆ **[Thread](#)**