

Re: can I use keep-state for icmp rules?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-10/6313.html>

From: David Trzcinski (xlr82xs@xlr82xs.shacknet.nu)

Date: 10/31/01

From: David Trzcinski <xlr82xs@xlr82xs.shacknet.nu>

To: freebsd-security@FreeBSD.ORG

Date: Thu, 1 Nov 2001 01:26:21 +1000

heh

this kinda makes me wonder why people use keep-state :P

```
ipfw add allow icmp from any to any out via <interface> icmptype 8
ipfw add allow icmp from any to <me> in via <interface> icmptype 0
```

will work fine for pings, just change the icmptypes to suit what you want to do...

you dont even need the outbound one if you allow all outbound traffic...

i dont use keep-state for my tcp either, with

```
ipfw add allow tcp from any to any out via <interface>
ipfw add allow log tcp from any to any 80 in via <interface> setup
ipfw add allow tcp from any to any in via <interface> connected
ipfw add deny log tcp from any to any in via <interface>
```

which, as far as i know should stop the problems mentioned with using keepstate..

if i'm wrong, please tell me :)

On Thu, 1 Nov 2001 01:01, Antonio Carlos Pina wrote:

> *Try again:*

>

> *ipfw check-state*

> *ipfw add allow icmp from {thishost} to any out via {oif} keep-state*

> *ipfw add deny icmp from any to any*

>

> *If your firewall is open by default, all packets will go thru. You have to*

> *got it closed by default or explicit deny the packets you don't want, as*

> *seen above.*

>

> *You should only ping the host back while the dynamic rule exists.*

FreeBSD-Security: Re: can I use keep-state for icmp rules?

>
> *Regards,*
> *Antonio Carlos Pina*
> *Diretor de Tecnologia (CTO)*
> *INFOLINK Internet*
> *<http://www.infolink.com.br>*
>
> ----- Original Message -----
> *From: "Michael Scheidell" <scheidell@fdma.com>*
> *To: <freebsd-security@freebsd.org>*
> *Sent: Wednesday, October 31, 2001 11:24 AM*
> *Subject: Re: can I use keep-state for icmp rules?*
>
>> ----- Original Message -----
>> *From: "Crist J. Clark" <crstjc@earthlink.net>*
>> *To: "Michael Scheidell" <scheidell@fdma.com>*
>> *Cc: <freebsd-security@freebsd.org>*
>> *Sent: Tuesday, October 30, 2001 7:42 PM*
>> *Subject: Re: can I use keep-state for icmp rules?*
>>
>>> *On Tue, Oct 30, 2001 at 07:39:09AM -0500, Michael Scheidell wrote:*
>>>> *You mean if I send email to your system, you can immediatly connect*
>>>> *to*
>>>
>>> *my*
>>>
>>>> *internal tcp ports that might not normally have external access*
>>>
>>> *available?*
>>>
>>>> *No. If you send out a TCP packet to my system that matches your*
>>>> *'keep-state' rule,*
>>>>
>>>> *TCP*
>>>> *src_ip.src_port -----> dst_ip.dst_port*
>>>>
>>>> *I can send _any_ TCP packet back,*
>>>>
>>>> *TCP*
>>>> *src_ip.src_port <----- dst_ip.dst_port*
>>>>
>>>> *And it will pass provided the source and destination IP and ports all*
>>>> *line up. ipfw(8) does not consider the TCP flags, sequence number,*
>>>>
>>>> *So, is ipfilter MORE statefull? ie, will it check more carefully?*
>>>> *One reason I asked, while testing the ipf icmp rules.*
>>>>
>>>> *Step 1: ipfw add allow icmp from {thishost} to any out via {oif}*
>>>>
>>>> *keep-state*
>>>>
>>>>

Re: can I use keep-state for icmp rules?

FreeBSD-Security: Re: can I use keep-state for icmp rules?

> > *Step 2: ping remote host*
> > *(works)*
> > *Step 3: log on to remote host and ping {thishost} back. I was able to*
>
> *ping*
>
> > *it.*
> > *Sorta scared me. (no additional ipfw rules)*
> >
> >
> >
> >
> >
> > *To Unsubscribe: send mail to majordomo@FreeBSD.org*
> > *with "unsubscribe freebsd-security" in the body of the message*
>
> *To Unsubscribe: send mail to majordomo@FreeBSD.org*
> *with "unsubscribe freebsd-security" in the body of the message*

--

Weird enough for government work.
To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message