

RE: [fw-wiz] Odd PIX / router behavior

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-10/0175.html>

From: Claussen, Ken (*Ken_at_kccweb.com*)

Date: 10/30/03

To: "Melson, Paul" <PMelson@sequoianet.com>, <firewall-wizards@honor.icsalabs.com>

Date: Thu, 30 Oct 2003 10:35:58 -0500

Paul,

I would venture to say that the loopback address is configured on the ISP's router one or two hops upstream from your Pix. It is clearly not locally defined since you cannot ping it when specifying the inside interface. On a Pix 515 DMZ bundle the DMZ interface defaults to this address, but you are using the 506 which only has two interfaces. I agree with your assessment based on the trip times, the 1605 cannot have this configured either. It is most likely being used for BGP touting stability by the ISP. This is a common tactic to avoid route flapping in the BGP Internet routing tables. I suspect it is within your ISPs network because this traffic is usually not passed between ISPs, in my experience. As you suggested you could add access lists on the 1605 outbound dropping the traffic, or you could add them on the Pix as well. However I would be curious to find out where the 127.0.0.1 traffic is actually being generated from. Dropping it via access list will stop it from being passed, but why is it there in the first place? Perhaps an internal machine's HOSTS file has been altered and this statement was removed, in which case the traffic would follow the default route. With some of the recent discussions about malicious HOSTS file entries, this seems like a plausible explanation. HTH.

Ken Claussen MCSE (NT42K) CCNA CCA

"In Theory it should work as you describe, but the difference between theory and reality is the truth! For this we all strive"

-----Original Message-----

From: Melson, Paul [mailto:PMelson@sequoianet.com]

Sent: Wednesday, October 29, 2003 5:18 PM

To: firewall-wizards@honor.icsalabs.com

Subject: [fw-wiz] Odd PIX / router behavior

Has anyone seen anything like this before?

```
pix# ping inside 127.0.0.1
```

```
127.0.0.1 NO response received --- 1000ms
```

```
127.0.0.1 NO response received --- 1000ms
```

```
127.0.0.1 NO response received --- 1000ms
```

RE: [fw-wiz] Odd PIX / router behavior

Firewall-Wizards: RE: [fw-wiz] Odd PIX / router behavior

The above is what I expect to get when I ping 127.0.0.1 from a PIX.

```
pix# ping outside 127.0.0.1
  127.0.0.1 response received --- 20ms
  127.0.0.1 response received --- 10ms
  127.0.0.1 response received --- 10ms
```

The above is *NOT* what I expected to get when pinging 127.0.0.1 from a PIX.

In this case, the PIX is a 506 running 6.1(4) and its outside interface is connected to a Cisco 1605 (IOS version unknown) via cross-over cable. Despite the responses, 127.0.0.1 never appears in the PIX's ARP table. I was thinking the router may be misconfigured:

```
# ping Y.Y.Y.Y
  Y.Y.Y.Y response received --- 0ms
  Y.Y.Y.Y response received --- 0ms
  Y.Y.Y.Y response received --- 0ms
```

That seems to rule out the router, since the response times are so different, and put the source of this traffic at least another hop or so away. At this point, I am at a loss for how or why this is happening. My next move will probably be to configure the 1605 with access-lists to drop reserved and special address ranges, but I'd really like to get to the bottom of this before I shut the door on it.

This investigation started when a customer began seeing spoofing messages in their firewall logs:

106016: Deny IP spoof from (127.0.0.1) to X.X.X.X on interface outside

My initial reaction was that the inside host that is statically NAT-ed to X.X.X.X was infected with MS-Blaster (<http://www.securityfocus.com/archive/75/335132/2003-08-21/2003-08-27/0>), but that's been ruled out.

Thanks,
PaulM

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

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