

## Re: [fw-wiz] Question about setting up PIX firewall

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2005-12/msg00003.html>

---

- *From:* "Paul D. Robertson" <[paul@xxxxxxxxxxxxx](mailto:paul@xxxxxxxxxxxxx)>
  - *Date:* Fri, 2 Dec 2005 02:18:06 -0500 (EST)
- 

On Fri, 2 Dec 2005, James wrote:

> I would strongly disagree Paul. We can learn an enormous amount of  
> recon intelligence from Matthews config.  
>

Well, I got several messages of support which said "I'm glad you said that  
so I didn't have to (those folks are welcome to chime back in,) so let's  
look at your points..."

> 1. We know he is using a PIX so we only have to look for exploits for that.

Assuming it's up to date, that leaves zero day exploits, which really  
should be rare these days. It also assumes the PIX is the only  
firewall there (which is likely, but not definite.)

> 2. Domain name-> domain-name spectrumdirect.local and dns server  
> vpngroup SpectrumDirect dns-server 192.168.1.250  
> 192.168.1.250  
>

Yes, we could probably derive that anyway- it's a .edu- it's not like  
their architecture is uber seekrit...

> 3. His rfc1918 subnet-> 192.168.1.128 255.255.255.128  
> Which we may be able to exploit with source routed packet attacks.  
> (I am not sure how well the PIX stands up to these)

If either strict or loose source routing gets through your firewall, it's a  
decade out of date... In any case, \*lots\* of people use outlook express  
or other things which "leak" 1918 addresses, that shouldn't matter one  
bit. Know what? My home network is 10.1.10.x/24- knowing that won't do  
you one bit of good, because my security implementation is as strong as  
it needs to be and my ruleset is protective..

>  
> 3. He is using a client to site vpn with split tunnelling enabled so if we could  
> find a users home PC and compromise it we could gain a significant  
> amount of access while the user is connected to the vpn.

Re: [fw-wiz] Question about setting up PIX firewall

>

But if you could find a client \*and\* compromise it, you'd be able to do that \*anyway\*, knowing the ruleset doesn't significantly change the risk there. FWIW, you'd have to find and compromise a VPN-allowed client and if you can do that, there are way more useful things you can do as an attacker with or without split tunneling. If you need split tunnels, you're likely not sophisticated enough an attacker to worry about the minor incremental risk.

> 4. We know the vpn config so we can easily get our hands on the cisco vpn client  
> and try to BF the password because the AUTH is LOCAL and the BF  
> attempt probably won't be detected.

If it's subject to a brute force, it is anyway- it's more likely that that would happen blind these days.

>

> 5. telnet 192.168.1.0 255.255.255.0 inside  
> Telnet is used to administer the box so if we can compromise the web  
> server inside we can  
> probably sniff the pix password and allow ourselves whatever access we want.

If you could do that, you'd be able to do the same thing anyway, the confing doesn't materially add to that- you'd still have to have an exploit. Of course, this assumes the network is sniffable, which is not a given these days. On a .edu network, an outside attacker isn't the likely point of compromise anyway.

> These are just a few ideas I pulled of the top of my head. Matthew  
> Davis if you are reading this I strongly advise you to request the  
> firewall wizards mailing list pull your post off their servers and  
> also request google to do the same however more than likely your post  
> has  
> already been cached and or skimmed.

Assuming your firewall is functional (and you've provided zero evidence that his isn't) then if your firewall ruleset isn't publically auditable, you're doing something wrong. If it is, then its disclosure adds very little to the actual risk.

Paul

---

Paul D. Robertson "My statements in this message are personal opinions paul@xxxxxxxxxxxxx which may have no basis whatsoever in fact."  
<http://fora.compuwar.net> Infosec discussion boards

---

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

Re: [fw-wiz] Question about setting up PIX firewall

- **References:**

- ◆ **Re: [fw-wiz] Question about setting up PIX firewall**

- ◆ *From: James*

- Prev by Date: **Re: [fw-wiz] Question about setting up PIX firewall**

- Next by Date: **[fw-wiz] [Administrivia] Backlog, Vacations...**

- Previous by thread: **Re: [fw-wiz] Question about setting up PIX firewall**

- Next by thread: **[fw-wiz] [Administrivia] Backlog, Vacations...**

- Index(es):

- ◆ **Date**

- ◆ **Thread**