

Re: Cisco PIX with SSH enabled on external port for maintenance

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-11/0305.html>

From: Cory Stoker (*cory_at_cleartnetsec.com*)

Date: 11/17/05

Date: Thu, 17 Nov 2005 15:18:59 -0700

To: security-basics@securityfocus.com

I took the original poster as wanting to enable SSH to the PIX itself for maintenance on the PIX.....

If this is the case then:

- PIX SSH does not support public key authentication. (At least I think so, how would this work on a PIX with a limited filesystem?)
- PIX OS versions below 7.0 do not support SSH version 2 which means that it has security issues.
- If you do not know the external IP addresses connecting to the PIX for maintenance you would have to open it to all which means that SSH brute forcing attempts would be possible. VPN fixes this by requiring you to authenticate to the VPN then to the PIX thereby alleviating the brute force issue by not having SSH available to the outside world.
- PIX supports VPN so what other hardware would there be? Of course you have to have a cryptographic license but I think these are free.
- PIX VPN's support split tunneling so you would not be disconnected.
- VPN also allows you to do other maintenance things like TFTP backup and SNMP querying. As far as the PIX SSH it is not as robust as OpenSSH so no tunneling through it like you do on a computer running OpenSSH. Also you have the ability to filter, log, and deny things from the VPN tunnel.
- Yes the VPN encrypts traffic so that is why you can telnet to the PIX after you VPN as telnet would be encrypted too by the VPN. However many deny telnet across the board so in that case you would VPN then SSH with the being double encrypted.....
- You could have a server available from the Internet with SSHD

SecurityFocus BASICS: Re: Cisco PIX with SSH enabled on external port for maintenance

running that then tunnels you to the PIX on the inside interface but this solution has a major flaw of having to go through the PIX first. What if you mess up the "static", "nat", or "access-list" on the PIX which means you are severed from the inside network from the Internet? Many times the PIX itself is available but nothing past it is in my experience. Plus you would need this server which is an extra item.

Thanks,

```
---
Cory Stoker
ClearNet Security
On Nov 16, 2005, at 3:09 PM, Alloishus BeauMains wrote:
> You can tunnel everything through SSH as well as VPN. VPN just closes
> down local network access if specified. VPN can use group
> authentication, but this seems to be just like an authentication key
> much like the one that SSH has.
>
> If you use an authentication key (This is an encrypted physically
> different file you have to load on your outside machines) and then an
> appropriate passphrase to go with it. SSH already encrypts the
> traffic, just like VPN.
>
> I am not sure how much VPN offers, additionally to this. Especially
> not for the money, since SSH (with SSHD) is completely free and can be
> loaded on any system.
>
> So, to me, it seems like you would be paying for, or supplying more
> equipment only to get the "disconnected from rest of LAN" portion of
> VPN.
>
> Anyhow, there is my take on it. You can make SSH as secure as you want
> it to be through those methods I mentioned.
>
> On 11/15/05, John Maher <john.e.maher@gmail.com> wrote:
>> -----BEGIN PGP SIGNED MESSAGE-----
>> Hash: SHA1
>>
>>
>> Chris Largret wrote:
>>> If you DO allow access to SSH to the outside world, there are a few
>>> things you can do to make it more secure:
>>>
>>> 1. Use a non-standard port
>>> 2. Use only the strongest algorithms that SSH supports
>>> 3. Change the passwords regularly
>>> 4. Allow only strong passwords
>>> 5. Limit which IP addresses can connect
>>
>> If feasible, I would recommend using public key authentication and
>> disabling password authentication.
>> -----BEGIN PGP SIGNATURE-----
>> Version: GnuPG v1.4.1 (GNU/Linux)
>> Comment: Using GnuPG with Fedora - http://enigmail.mozdev.org
>>
>> id8DBQFDeknduY7WcSII22oRAqCHAJ0cidbUKqRm4qUKzu/8buP/62haAgCcDJhf
>> H7mx4DzKwoJz01a/R6gVN+M=
>> =r+xe
```

SecurityFocus BASICS: Re: Cisco PIX with SSH enabled on external port for maintenance

```
>> -----END PGP SIGNATURE-----  
>>  
>
```