

[fw-wiz] Followup: An interesting VPN problem

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-09/0008.html>

From: Jonas Anden (*dajudge_at_home.se*)

Date: 09/01/03

To: firewall-wizards@honor.icsalabs.com

Date: 01 Sep 2003 17:51:08 +0200

Thanks for all replies. I'll try to summarize them all here to share our findings.

- Source routing cannot be done on the PIX (at least not on the 501 model).

- Normal routing rules can be used to accomplish the desired effect:

- Put the default route on the inside:

```
route inside 0.0.0.0 0.0.0.0 192.168.20.1
```

- Add a host route for the remote PIX:

```
route outside 10.10.0.2 255.255.255.255 10.0.0.1
```

- Repeat above steps for the remote PIX, (of course changing IP addresses as necessary).

- Add a network route for the remote network on the local PIX:

```
route outside 192.168.21.0 255.255.255.0 192.168.21.1
```

This has the desired effect; all traffic on the remote network is pushed through the tunnel and routed through the local firewall.

One comment though: I'm also using dhcp relaying for the IP address assignments. Strange enough; the relayed DHCP does **not** go through the tunnel (bypassing routing rules). So I had to set up a two-step relaying; the remote pix relays to the external IP of the local pix, which has relays into the local dhcp server.

Thanks for all your help!

// J

On Thu, 2003-08-28 at 10:27, Jonas Anden wrote:

Firewall-Wizards: [fw-wiz] Followup: An interesting VPN problem

> *Hi all you Wizes out there. I've got a bit of a problem that I think you
> might help me solve...*

>

> *I've got two Cisco PIX 501 with the latest software (6.3.1). We're
> trying to use them to set up a remote site with *all* client traffic on
> the remote network being redirected through the site-to-site tunnel
> (including the traffic that should ultimately end up on the Internet).
> Traffic from the remote network not targeted for the local network
> should be routed through a firewall reachable from the local network.*

>

> *My network looks like this:*

>

>

> *[L-NET]<-+---->[FW]<----+-->[B-GW]<-->[INET]<-->[R-PIX]<-->[R-NET]*

> *||*

> *+-->[L-PIX]<-+*

>

>

> *L-NET – The network at the central site*

> *Net=192.168.20.0/24*

>

> *FW – Firewall protecting the entire network and*

> *providing user authentication for Internet access.*

> *Inside IP=192.168.20.1*

> *Outside IP=10.0.0.2*

>

> *L-PIX – Local tunnel endpoint at the central site.*

> *Connected to both the internal network at*

> *the central site and the Internet.*

> *Inside IP=192.168.20.2*

> *Outside IP=10.0.0.3*

>

> *B-GW – Border gateway of central site.*

> *IP=10.0.0.1*

>

> *INET – Internet*

>

> *R-PIX – PIX as border router of remote network.*

> *Inside IP=192.168.21.1*

> *Outside IP=10.10.0.2*

>

> *R-Net – Remote network.*

> *Net=192.168.21.0/24*

>

> *Now, what I want to do is first set up a tunnel between the two networks*

> *(L-NET and R-NET). Computers on L-NET has a default gateway of*

> *192.168.20.1, accessing Internet through FW. FW Provides access control*

> *for these users. FW also has a static route to route traffic to R-NET*

> *through the L-PIX.*

>

> *Computers on R-NET has the PIX inside IP (192.168.21.1) as the default*

Firewall-Wizards: [fw-wiz] Followup: An interesting VPN problem

> gateway. All their traffic (including the traffic that should end up on
> the Internet,) should be transmitted through the tunnel. For the client
> traffic exiting the tunnel on L-NET, there needs to be a default gateway
> set to 192.168.20.1, so that their Internet traffic also exits through
> FW, and FW can provide access control for these users.
>
> It is absolutely vital that the traffic does not exit directly to the
> Internet at either PIX. All client traffic bound for the Internet *must*
> be routed through the firewall at the central site (FW).
>
> I've managed to set up a Site-to-Site VPN between the two PIXes,
> establishing network connectivity between the two networks, but I have
> found no solution to applying a default gateway for the traffic going
> from the remote network to Internet. The traffic needs to be
> source-routed in some way, or the clients on the remote network will not
> be able to access the Internet (or any of the other routed networks I've
> got set up here) at all.
>
> Is this at all possible to do with two PIXes? As far as I can tell, the
> remote PIX is doing what it should; forwarding *all* traffic through the
> tunnel. But the local PIX doesn't know what to do with the packets to
> the Internet, so it just drops them.
>
> If this is not possible with the PIXes, could anyone recommend a
> solution? I've done experiments with a Linux box with FreeS/WAN and got
> that to work (using source routing), but I'd like to use a peripheral
> for this job.
>
> //J
>
>
>

> 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>