

Re: [fw-wiz] bypassing PIX limitation

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-11/msg00025.html>

- *From:* Paolo Supino <paolo@xxxxxxxxxxxxxxxx>
 - *Date:* Fri, 10 Nov 2006 10:57:16 -0500
-

Hi Kevin

That is what I thought of doing but I can't find any documentation on how to do it. Can you please direct me to documentation that show's how to NAT traffic going into a VPN?

TIA
Paolo

Horvath, Kevin M. wrote:

In this case you could just try to nat the traffic through the vpn&.haven t tried it before but it should work.

Kevin

From: firewall-wizards-bounces@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
[<mailto:firewall-wizards-bounces@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>] *On Behalf
Of *David Swafford
Sent: Thursday, November 09, 2006 2:16 PM
To: firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Subject: Re: [fw-wiz] bypassing PIX limitation

Hi Paolo,

In your existing network, are you using any of the 172.28.x.x address space? If not, then one option that comes to my mind is that you could setup another Pix box who's sole purpose is to connect to the partner's tunnel (if the traffic is not too demanding maybe something small like a PIX 506?) I would then suggest that you somehow propagate a route that points to the PIX as being the next hop gateway for all 172.28.x.x addresses. This most likely involves the need to purchase another PIX or maybe just setting another interface on a cisco router

Re: [fw-wiz] bypassing PIX limitation

running the IOS firewall would work?

Just a few thoughts.

David Swafford.

Hi Kevin

The IP address space assigned to me is not part of their public IP address space. I apologize, I explained myself wrong. Hopefully the following information will be clearer: The network behind my PIX is 192.168.99.x (the pix has a public IP address). Our partner uses IP addresses on network 172.28.x.x/16. They want me to use on my network IP addresses on subnet 172.28.150.32/28.

TIA
Paolo

Horvath, Kevin M. wrote:

When you say carved out of their IP network, I assume you are

talking about

the public assigned IP space, as the private ip space is anyone's. If

this

is correct then whoever wrote their policy needs to go to some basic

routing

training as that just doesn't make any sense. You should be able to nat traffic across a vpn tunnel, although I have never tried it, since

nat is

Re: [fw-wiz] bypassing PIX limitation

done before packets are encrypted. Your problem will be that you have to assign the outside ip block from the partner to your global

statement which

will probably give you issues, as it breaks routing concepts

(meaning those

aren't assigned/routed to you so they wont go anywhere, but since

they are

going over an ipsec tunnel its plausible). Even if you get it

working from

your side it will be interesting to see how they handle their incoming public ip space from an ipsec tunnel since its routed to their outside interface already. The more and more I think about this the more I

realize

it should not even be tried. Its just a bad idea altogether. I just hope you mean private ip not the partners public ip space when you say "

carved

out of their overall IP network range"?

Kevin M. Horvath
CISSP, CCSP, GCIH, INFOSEC, CQS-FW, CQS-VPN,
CQS-IDS, CCNA
SAIC - IT Security Division
703.868.1503

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

From:

firewall-wizards-bounces@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

<mailto:firewall-wizards-bounces@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

[\[mailto:firewall-wizards-bounces@xxxxxxxxxxxxxxxxxxxxxxxxxxxx\]](mailto:firewall-wizards-bounces@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

On Behalf

Re: [fw-wiz] bypassing PIX limitation

Of Paolo

Supino

Sent: Wednesday, November 08, 2006 7:23 PM

To: Firewall Wizards Security Mailing List

Subject: [fw-wiz] bypassing PIX limitation

Hi

I have a network that is protected by a PIX 515e running 6.3(1). I was asked to setup a IPSEC VPN with a partner. The partner's security

policy

mandates that a remote encryption domain must use IP addresses on a subnet carved out of their overall IP network range. The network behind my PIX uses IP addresses on a subnet that is outside of their IP network. Adding a second IP to my network isn't supported by the PIX

OS.

To bypass this limitation I thought of NATing packets going into the

VPN

tunnel. I've been looking for documentation for such a scenario, but can't find anything. Can packets going into a VPN tunnel be NATed?

TIA
Paolo

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxx

[<mailto:firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxx>](mailto:firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxx)

Re: [fw-wiz] bypassing PIX limitation

Re: [fw-wiz] bypassing PIX limitation

<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

<<mailto:firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>>

<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
<<mailto:firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>>
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

Founded in Faith – Preserved with Pride – Sustained by Spirit

Upcoming Events:
ALTER OPEN HOUSE
November 16
7 – 9 p.m.

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

Re: [fw-wiz] bypassing PIX limitation

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>