

RE: [fw-wiz] Pix to Pix VPN IPSec w/ PAT

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-03/0069.html>

From: Brian A Kee (bkee@lurhq.com)

Date: 03/24/03

From: "Brian A Kee" <bkee@lurhq.com>
To: <david@zbonski.com>, <firewall-wizards@honor.icsalabs.com>
Date: Mon, 24 Mar 2003 12:16:21 -0500

Here is an example:

```
# Define a global/nat setting for the traffic you want to use PAT (in this
case we define the external interface IP as the translation IP). We then
define what traffic we want to avoid the nat rules (nat 0) so that
everything jives through the tunnel. We then setup a normal nat rule for all
traffic destined for the all other destinations except the VPN Network.
global (inside) 10 interface
nat (inside) 0 access-list NAT_0
nat (inside) 10 192.168.1.0 255.255.255.0

# define our allowed outbound services to the internet.
access-list INSIDE permit ip object-group InternalNet any object-group
Allowed_SVC

# define the traffic that we want to encrypt
access-list CRYPTO permit tcp object-group InternalNet object-group VPNNet
object group Crypto_SVC

# define the traffic that we do not want to nat (see nat 0 rule above)
access-list NAT_0 permit tcp object-group InternalNet object-group VPNNet
object group Crypto_SVC

# Define your rpyto map entries for the tunnel using the match address
statement to define what traffic is encrypted.
crypto map VPN 20 ipsec-isakmp
crypto map VPN 20 match address CRYPTO
crypto map VPN 20 set peer CryptoHost
```

I hope this helps!

BAK

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

From: firewall-wizards-admin@honor.icsalabs.com
[mailto:firewall-wizards-admin@honor.icsalabs.com] On Behalf Of David

RE: [fw-wiz] Pix to Pix VPN IPSec w/ PAT

Firewall-Wizards: RE: [fw-wiz] Pix to Pix VPN IPsec w/ PAT

Zbonski

Sent: Monday, March 24, 2003 11:03 AM

To: firewall-wizards@honor.icsalabs.com

Subject: Re: [fw-wiz] Pix to Pix VPN IPsec w/ PAT

I know you can reserve static addresses to use, so that you can do PAT for other clients and still do IPSEC with a different address. You will need 2 (or more) IP addresses from your cable modem provider – which you should be able to get with a business class connection.

You probably can PAT the IPSEC traffic – I know for sure that you can do it on a regular router with one public IP address by creating a loopback – I just don't know the exact commands to do it on a PIX. Do you have one or more IP addresses to work with?

David Zbonski

Zbonski Consulting

<http://www.zbonski.com>

>Hey all.. newbie to the list here.. but I have a question for you all.

>

>I've looked everywhere, and my cisco rep has yet to get back to me..

>

>Is it possible to perform a CISCO pix501 to pix501 VPN w/ IPsec while still

>utilizing PAT. The scenario is = Business Cable Modem to Business Cable

>Modem... thoughts?

>

>Thanks a bunch,

>Paul Matuszewski

>Systems Administrator

>In Office Networks

>(305) 799-4871

STOP MORE SPAM with the new MSN 8 and get 2 months FREE*

<http://join.msn.com/?page=features/junkmail>

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>

RE: [fw-wiz] Pix to Pix VPN IPsec w/ PAT