

Re: Risks associated to branch office IPSec devices

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-06/0214.html>

From: Matt Bellizzi (matt.bellizzi_at_nokia.com)

Date: 06/22/05

Date: Tue, 21 Jun 2005 18:20:55 -0700

To: Rodrigo Blanco <rodrigo.blanco.r@gmail.com>

Hey

Most VPN appliances have what are called selectors. I believe per RFC are bypass, encrypt or drop. If the traffic matches the selector then just like a firewall rule it will do whatever the selector specifies. If the IPSec gateway default is to bypass all non-encrypted traffic that would be bad. Personally if the VPN device is locked down properly and has anti spoofing code implemented and only allows udp 500 and AH or ESP I really see no need for a firewall as long as default behavior for non-encrypted traffic is drop. As for the NAT portion are you talking about NAT before IPSec or are talking about VPN GW just NAT'ing out bound traffic that matches no encrypt selector?

Matt Bellizzi
Nokia Enterprise Systems
SQA Engineer IP VPN Group

ext Rodrigo Blanco wrote:

>Hello list,
>
>I have just come across a doubt about branch office VPN devices.
>Normally, they are used so that a branch office's network – typically
>with a private addressing scheme – can securely connect to the
>headquarters' central network.
>
>Such VPN devices normally do not include a firewall, so I was
>wondering if this really represents a risk:
>
>Yes – it is a risk if the VPN device just acts as a router (no ACLs)
>and is attached to the Internet.
>No – because the addressing scheme behind it is private, hence
>non-routable, hence unreachable across the Internet (internet routers
>would drop packets with such destinations?)
>

SecurityFocus Penetration: Re: Risks associated to branch office IPSec devices

>*The only real risk I see is if the VPN device is cracked, and from
>there the security of the whole network (both brach office and
>headquarters) is exposed. Am I right?*

>

>*Any ideas would be more than welcome. Thanks in advance for your
>advice and best regards,*

>

>*Rodrigo.*

>

>

>