

Re: Linux v Dedicated NAT routers – secure remote differences

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/10282.html>

From: Leonid Rosenboim (MY_FIRST_NAME@CONSULTANT.COM)

Date: 09/29/02

From: "Leonid Rosenboim" <MY_FIRST_NAME@CONSULTANT.COM>

Date: Sun, 29 Sep 2002 18:46:18 +0200

Alan,

I think I have got the core of the issue, I assume you are using an IPsec VPN, so here is a quote from a Cisco paper on VPNs:

NAT After IPSec

...

When IPSec uses Authentication-Header (AH) mode for packet integrity, if one-to-one address translation occurs it will invalidate the signature checksum. Because the signature checksum is partially derived based on the AH packet's IP header contents, when the IP header changes, the signature checksum is invalidated. In this case, the packet will appear to have been modified in transit and will promptly be discarded when received by the remote peer. However, when IPSec uses ESP, the devices will be able to successfully send packets over the VPN, even when one-to-one address translation occurs after encapsulation. This scenario is possible because ESP does not use the IP header contents to validate the integrity of the packets. In cases where many-to-one address translation occurs (aka port address translation), the IP address and source IKE port, normally User Datagram Protocol (UDP) port 500, will change. Some VPN devices do not support IKE requests sourced on ports other than UDP 500, and some devices performing many-to-one NAT do not handle ESP or AH correctly. Remember that ESP and AH are higher-layer protocols on top of IP that do not use ports.

Because many-to-one address translation is commonplace in many environments where remote-access clients are deployed, a special mechanism called NAT transparency exists to overcome these NAT issues. NAT transparency reencapsulates the IKE and ESP packets into another transport layer protocol, such as UDP or TCP, which address-translating devices know how to translate correctly. This mechanism also allows the client to bypass access control in the network that allows TCP or UDP but

comp.security.firewalls: Re: Linux v Dedicated NAT routers – secure remote differences

blocks encrypted traffic. Note that this feature does not affect the security of the transport in any way. NAT transparency takes packets already secured by IPSec and then encapsulates them again in TCP or UDP.

Full