

RE: [fw-wiz] IPSEC over load-shared T1s (per packet)

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-09/0078.html>

TSimons_at_Delphi-Tech.com

Date: 09/19/03

To: ben@iagu.net

Date: Fri, 19 Sep 2003 08:18:51 -0400

Thanks Ben, the RJ's are clean, I chewing on them to make sure :-)
anyway...both circuits work fine individually.

I talked to someone on another mailing list and they said they had the same problem, but switching from PER-PACKET load sharing to PER-DESTINATION cleaned things up.

At this point I have a ticket open with the firewall vendor (SEF) and have provided them countless traffic dumps, they probably hate me :-), I hope to resolve this by this weekend. The info you provided about sequencing is a great help, and makes perfect sense. When I combine the TCP traffic dumps with the ESP traffic dumps the ratio of ~1 to ~1 definitely does not hold true when both T1s are active.

Another theory that someone had was the CRC was failing because the packets are taking different routes, but I get no errors in the firewall. ...I really want to discount this theory because the T1s terminate in the same router here and at the NOC, so the count hop and speed is exactly the same, and the last hop tag on the packet will be the F0/0 interface of the router anyway.

....the quest continues....

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

From: Ben Nagy [mailto:ben@iagu.net]

Sent: Thursday, September 18, 2003 4:41 PM

To: TSimons@Delphi-Tech.com; firewall-wizards@honor.icsalabs.com

Subject: RE: [fw-wiz] IPSEC over load-shared T1s (per packet)

ObBOFH: One of the T1 RJ connectors must be dirty, which is causing packet corruption. Give both the telco jacks a good clean (licking them works well) and see if that fixes the problem. [1]

Seriously, I do have a theory ;)

Firewall-Wizards: RE: [fw-wiz] IPSEC over load-shared T1s (per packet)

Does this routing guarantee to preserve sequencing?

If it's really as you described (packets send one for one via alternate links) then you have some potential problems brewing, I think.

TCP will "work things out" when packets arrive out of sequence, but with IPsec it's left up to the implementation. One security concern with most crypto things is replay protection. IPsec addresses this by using a mandatory sequence number in the ESP header. The receiving IPsec doesn't have to take any notice, but most do. If your receiving IPsec has enabled replay protection then if one link is going faster half the packets are going to get dropped (sequence number < current).

This would make your tunneled protocol (say TCP) do the retransmission thing, so it would work itself out eventually, but the speed would indeed suffer horribly.

See if you can convince your router to preserve "IP flows" and use the two links in a more sensible manner. That might help.

Best of luck,

ben

PS: Let us know when you work it out? This is an interesting one.

[1] The RJ's are live, for non-network-engineer types. Not enough to kill you, but it hurts. :)

> -----Original Message-----
> From: firewall-wizards-admin@honor.icsalabs.com
> [mailto:firewall-wizards-admin@honor.icsalabs.com] On Behalf
> Of TSimons@Delphi-Tech.com
> Sent: Thursday, September 18, 2003 3:38 AM
> To: firewall-wizards@honor.icsalabs.com
>
> Hello All
>
> Recently we doubled our internet bandwidth to two T1s from the
> same provider
> that terminate on in the same router on the NOC side.
>
> We setup IP LOAD-SHARING PER-PACKET on each of the serial
> links on both
> sides (NOC and Us) in order to get an aggregate 3.0mbit.
> PER-PACKET routing
> alternates usage of the T1s, one for one...
>
> Since then, VPN performance has taken a dive. Sniffing out
> traffic, ESP
> packets are sent 3-4 times before they can be properly decrypted.

RE: [fw-wiz] IPSEC over load-shared T1s (per packet)

Firewall-Wizards: RE: [fw-wiz] IPSEC over load-shared T1s (per packet)

- >
- > *Someone along the way said that using PER-PACKET routing*
- > *changes the CRC*
- > *value of the packets. Is this correct, has anyone else seen*
- > *this issue? I*
- > *can't see how the CRC is changed, the hop count isn't*
- > *changing, the lines*
- > *are identical, and they terminate in the same router, so the*
- > *last hop is the*
- > *F0/0 interface of the router before getting to the firewall.*
- >
- > *Thanks,*
- > *~Todd*
- >
- > _____
- > *Todd M. Simons*
- > *Senior MIS Engineer*
- > *Dell Tier 1 PA Technician*
- > *Delphi Technology, Inc.*
- > *New Brunswick, NJ*

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>