

Re: Transport Mode IPSEC

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2007-01/msg01517.html>

- *From:* "Ted Mittelstaedt" <tedm@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 18 Jan 2007 01:25:44 -0800
-

You don't trust your own switch?

Your making a common mistake here. Your confusing application security with environment security. If an environment is insecure you cannot make it secure by mucking with the application. (ie: hiding it in a tunnel)

for example you cited arp cache poisoning on an ethernet network. running ipsec will not protect against this. If your ethernet environment is insecure (ie: your using unmanaged switches) and it's got hostiles on it, you can run all the ipsec you want, an attacker can DoS your NFS server with an arp cache poison, no problem. Or, assume the MAC of your default gateway and knock all users offline.

If you correct the environment security, then the application is protected. For example, you put in a decent managed switch, you setup rate-limiting on it, you setup MAC/IP address filters, and your now secure on your local LAN.

Basically, what your trying to do – use ipsec to encrypt nfs on a local lan – is unnecessary, adds overhead, and what you want to have happen is better done by other mechanisms.

If your running NFS over a WAN connection where ipsec encryption would have some validity, well, NFS isn't a good protocol for such a connection. Copying a file is going to be slow. WANs are unreliable and you don't want your NFS mounts vanishing without being unmounted. sftp would be a much better choice I think.

NFS isn't inherently insecure unless it's improperly deployed. I would consider deploying NFS on a hostile ethernet network that is not secured, to be an improper deployment and I think any security professional would agree.

This discussion is like when Microsoft made packet signing mandatory in SMB in Windows XP. They said "this will enhance the security of SMB" No it didn't. SMB packets in Real Life are almost always on a local LAN, and most of those are switched. All that did is break

Re: Transport Mode IPSEC

connecitons to UNIX Samba servers (which was probably the real reason they did it)

Ted

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

From: "Dan Mahoney, System Admin" <danm@xxxxxxxxxxxxxxxx>

To: "Ted Mittelstaedt" <tedm@xxxxxxxxxxxxxxxx>

Cc: <questions@xxxxxxxx>

Sent: Thursday, January 18, 2007 12:06 AM

Subject: Re: Transport Mode IPSEC

On Wed, 17 Jan 2007, Ted Mittelstaedt wrote:

Dan,

You do realize, don't you, that since both of these hosts are on a switch,

and are using unicast traffic to communicate with each other, that they cannot be sniffed, don't you?

That implies trust of the switch, trust against arp-cache poisoning, and the like. The idea of ipsec is not trusting the wire.

With NIS/NFS known for being this inherently secure, would it get me a better answer if I said "with only a single router between them"?

-Dan

--

-----Dan Mahoney-----

Techie, Sysadmin, WebGeek

Gushi on efnet/undernet IRC

ICQ: 13735144 AIM: LarpGM

Site: <http://www.gushi.org>

freebsd-questions@xxxxxxxx mailing list

Re: Transport Mode IPSEC

Re: Transport Mode IPSEC

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@xxxxxxxxxxxxx"