

Re: IPSEC Certificate

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.vpn/2008-04/msg00029.html>

- *From:* "Phillip Windell" <philwindell@xxxxxxxxxxx>
 - *Date:* Fri, 18 Apr 2008 13:21:49 -0500
-

"Hutch" <Hutch@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:F57F163F-95A1-47BF-BEB3-497C86FA32BC@xxxxxxxxxxxxxxxxxxxx>

Ok..I have a RRAS server running internally, and have used the pre-shared key before...but would rather go the Cert route.

Sure, that's fine.

With PPTP isn't the username\password sent clear text??

No. That is Basic Authentication and FTP

Just the MS Dialup component by itself uses by default CHAP, MS-CHAP, or MS-CHAP v2. I think it just depends on what the device "answering" the call is capable of. So it is a Challenge/Response method,...meaning the password is never sent over the connection,..let alone in clear text. It is also capable of PAP [unencrypted] or SPAP, but those are not the defaults. Look in the properties of your Dialup Connection on the Client,..on the Security Tab, the default is "Require secured password" and "Require data encryption" regardless of the Protocol. If you go into the Advanced Settings you will see what I described above.

PPTP and L2TP both are encapsulated with encrypted packets. That is why even with PPTP you have to "break" the packets to see what is protected inside the encapsulated packets.

L2TP uses an additional layer of encryption on top of that, but I'll admit that I don't know nor can I explain the exact details of it.

We need to have the connection fully encrypted from login to logoff....so I thought L2TP was the better way to go.

Re: IPSEC Certificate

L2TP has deeper security,...but that does not mean the PPTP is "insecure".
That was really all I am trying to say. Do not confuse PPTP with the clear
text authentication of Basic Auth and FTP.

—
Phillip Windell
www.wandtv.com

The views expressed, are my own and not those of my employer, or Microsoft,
or anyone else associated with me, including my cats.
