

Re: IPsec questions

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-10/0273.html>

From: Steven L Umbach (*n9rou_at_nospam-comcast.net*)

Date: 10/21/05

Date: Fri, 21 Oct 2005 12:47:09 -0500

Transport mode is used for host to host traffic. Tunnel mode is used when one endpoint is a gateway [not the endpoint computer] and is mostly used to use ipsec over the internet with either certificate or preshared key authentication [best used for testing]. A common use of tunnel mode is when Ipsec endpoint devices are used like those you can buy from Netgear, Linksys, etc. The traffic is protected by ipsec only between the two endpoint devices where in transport mode the traffic is protected from computer to computer. Transport mode with kerberos authentication for computers is what is used when you configure an ipsec policy for the domain. The link below explains more. --- Steve

<http://www.microsoft.com/technet/security/topics/architectureanddesign/ipsec/ipsecapa.mspx>

"Chris Hall" <someone@microsoft.com> wrote in message news:eDva1Da1FHA.1028@TK2MSFTNGP12.phx.gbl...

> *Greeting,*

>

> *I realize this isn't a 'Certification' forum, but would like the*

> *thoughts/expertise of those in the Real World.*

>

> *I'm preparing for 70-214 and have some questions on IPsec and it's use in*

> *a*

> *network. IPsec runs in two modes, tunnel and transport. Can someone give*

> *me*

> *examples of when and why to use each? It seems to me that tunnel mode*

> *would*

> *be best served if using it to connect to servers like two exchange servers*

> *or an IIS to SQL server, where the endpoint was just that....the endpoint!*

>

> *Thanks in advance!*

> *Chris*

>

> *PS Now that I think about it, we run a lot of telnet traffic (read: clear*

> *text). Perhaps this would be a good implementation, as this application*

> *runs*

> *across our entire lan/wan infrastructure.*

>

>