



WAN Encryption: Just Do It

Posted by Mike Fratto, Editor on June 2, 2010

One of my philosophy professors asked the question "Where is your car parked?" I told him where I parked it. He then asked me how I knew it remained where I left it. "Is it possible," he asked, "that a group of pranksters picked it up and moved it elsewhere?" I'd pulled that prank, so I knew it was possible. Then he asked, "What if one set of pranksters moved your car elsewhere, and then another set of pranksters moved back to the spot where you left it by coincidence? Would I know?" The exercise goes right to the heart of network security. What assurances do you have that what you expect to happen is actually happening? One of the ongoing issues with wide area networking is how secure is secure enough? Once the data leaves your network, you have no idea what happens to it. If it leaves unencrypted, you have no idea if anyone snooped on it.

If you talk to the WAN services folks at a carrier, their definition of a VPN will be an overlay network that is carried by another network over shared infrastructure. By the carrier's definition, a telephone call over a PSTN is a VPN. The carrier definition is very different than the other definition of a VPN as an authenticated and encrypted layer 3 tunnel between two nodes, with one node being a network. The former definition assumes that the carrier's employees are trustworthy. The latter definition doesn't care if they are or aren't.

The telephone example might be silly, but it fits. However, carriers talk about frame relay or MPLS VPNs all the time, and if you think they're secure, you're mistaken. What they mean by secure is that the employees aren't going to snoop on the traffic, that the traffic is segregated from other traffic using well known layer two and three technologies, and that the carrier has a set of processes in place to ensure that unauthorized data or service manipulation won't take place. I'm not saying carriers aren't trustworthy and that your unencrypted frame relay or MPLS VPN will be snooped upon. I am saying that you have no assurance that it hasn't been snooped on by anyone, hence, the need for encrypting the traffic before it hits the WAN.

This should be standard operating procedure, but I still hear from IT admins in different verticals and different size companies who transmit potentially sensitive data unencrypted over the carrier's definition of VPN. Requirements like PCI and HIPAA have helped drive home the need for network encryption, but from the IT admin's point of view, they trust the carrier to protect their bits. I think the people who work in and on the carrier's network are probably trustworthy people who aren't bent on committing crimes of opportunity against the vulnerable, but I have no assurance that is the case. Worse, how would I know if someone was snooping on my traffic?

The cost to encrypt data whether in a layer 3 VPN or a layer 2 encryption is cheap nowadays compared to other IT purchases. Encryption performance has gotten to the point where network encryption is not a bottleneck or a hindrance to network operations, provided encryption is the last process before a packet enters the WAN and the first process when a packet comes from the WAN. In fact, even IP header information like QoS marking can be transferred from the encrypted packet to the external packet so that carrier-based shaping can be enforced. Whether you manage your own VPN encryption, or outsource it to a service provider, there is no reason not to encrypt data whether it goes over the Internet or your carrier's VPN service.

[Copyright 2009 United Business Media LLC, All rights reserved.](#)