Inside the VPN Tunnel

by Jeff Crume

Consulting Internet Specialist

IBM Advanced Technical Support

crume@us.ibm.com

Abstract

Along with the exciting upside of Virtual Private Networks (VPNs) comes some additional considerations, such as manageability and interoperability issues, that must be dealt with. Nevertheless, with potential savings estimates of 20%-80% over existing private network connections, many businesses are deciding that the increased complexity is well worth the hassle. The bottom line, though, is that despite its inherent complexities, the potential cost savings (as compared to dedicated lines) and security benefits of VPN solutions are more than enough to justify a long, hard look at this important technology. This article takes a look at VPNs and what makes them tick..

Is that the proverbial light at the end of the tunnel . . . or train? If you're talking about Virtual Private Network (VPN) tunnels, then it all depends upon your perspectiv

VPN technology carries with it the promise of cheap, secure, ubiquitous bandwidth. In other words, you could g anywhere in the world and still have access to your corporate network without destroying your IT budget in t process. Or you could connect to remote branch offices or even business partners over a public network, such as the Internet, and still keep your communications out of the rea of snooping competitors. Sound interesting?   So what's th catch, you may be wondering? It turns out that along with exciting upside of VPNs comes some additional considerations, such as manageability and interoperability issues, that must be dealt with. Nevertheless, with potential savings estimates of 20%-80%[1] over existing private network connections, many businesses are deciding that the increased complexity is well worth the hassle. So, let's take a look at what a VPN is and what makes it tick …

VPN Defined

What is a Virtual Private Network? Let's take the terms in reverse order. We know that a **network** is a series of connections that make it possible for us to send data from point A to point E In this context, "**private**" means that those communications can be read only by thei intended recipients. Private networks are nothing new, however. The trouble with them is that they are expensive. The network service provider has to dedicate

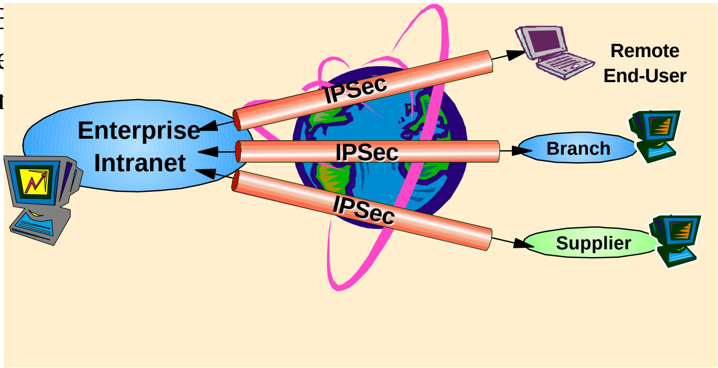

Figure 1. VPN Solutions

[1] "Virtual Private Networks: A Partnership Between Service Providers and Network Managers," Infonetics Research, Oct. 1997

the bandwidth to you, so they also have to pass along all of the costs to you as well. Figure 1 illustrates some possible VPN solutions.

That's where the "virtual" part comes in. If you could use public, shared bandwidth but maintain the security of a private, dedicated network, then your network service provider could spread the costs out among multiple customers and you wouldn't be stuck footing the entire bill. So, instead of "real" private network, you set up a "**virtual**" private network over a shared infrastructure. It seems to you just like the real thing — only at a fraction of the cost. In a sense it's like carving out a secure tunnel for your private communications through the public Internet.

Virtual Privacy or Virtually Private?

But how can you send a private message to a business partner over a public network? Public networks are for public information, right? Not necessarily.

If you send a postcard through the mail, you can't expect a great deal of privacy because anyone that sees your postcard can easily read what you've written on it. It's likely that only a few people, such as postal workers, would have access to the card while it's being delivered but, needless to say, this would not be the preferred method for sending corporate secrets.

Putting that postcard in an envelope, however, would certainly help. This way a snooper would have to actually open the envelope in order to steal your secrets. Of course, opening an envelope isn't a difficult thing to do, but if that envelope was made out of reinforced steel and secured with a combination lock whose code was known by only you and the recipient, then you could reasonably expect that your secret would be safe.

Unfortunately, you can't put your IP packets in a locked, steel-reinforced envelope before sending them over the Internet, but you can do the next best thing -- encrypt them. You could scramble the message before sending it to make sure that only the intended receiver knows how to unscramble it. This way, even if snoopers do   intercept the message, they can't make any sense out of what they intercepted.

Standards, Standards Everywhere ...

The key, to making all of this work, of course, is that the sender and receiver must know how to read these modified packets. Otherwise, the whole scheme falls apart. In order to do this, both sides must use the same encryption algorithm, know the appropriate encryption/decryption keys, and know the exact format of the modified packets. That's where standards help.

Standards are a wonderful thing -- which is why it seems everyone has one of their very own. VPN standards are no different. A number of competing and complementary tunneling options are available to choose from. It's very important to understand what each is capable of (and not capable of) so that you can choose the right one for your particular needs. One way to classify these alternatives is by the layer of the communications stack that they target.

Layer 2 Standards

The advantage of operating at the network interface layer (Layer 2) of the stack is that you gain a greater degree of protocol independence. For example, the traffic that a Layer 2 tunnel can carry includes IP, NetBIOS, IPX, and SNA because layer 2 is oblivious to the data being carried at the upper layers. This makes Layer 2 solutions ideal for achieving ubiquitous access over a single protocol backbone, such as the Internet, which runs over IP. This means that with a Layer 2 tunnel, you could dial into the Internet from a remote location and still connect to your LAN server running IPX or NetBIOS (or to your mainframe running SNA). In this case, the tunnel you have created is effectively encapsulating the higher level protocol inside an IP packet so that it can run over the IP-based Internet.

Proprietary protocols such as L2F (Layer 2 Forwarding) from Cisco and PPTP (Point-to-Point Tunneling Protocol) from Microsoft are two such examples. L2TP (Layer 2 Tunneling Protocol) represents a collaboration of these tw efforts into an open, IETF specification[2]. However, it can argued that L2TP is not a VPN standard in the strictest sense of the word, since it lacks a native means for sending data privately. In other words, the "P" in VPN is missing. L2TP makes up for this, though, when it is used in conjunction with IPSec (Internet Protocol Security), a Layer 3 standard, which does provide privacy. Figure 2 positions VPN options by networking layer.

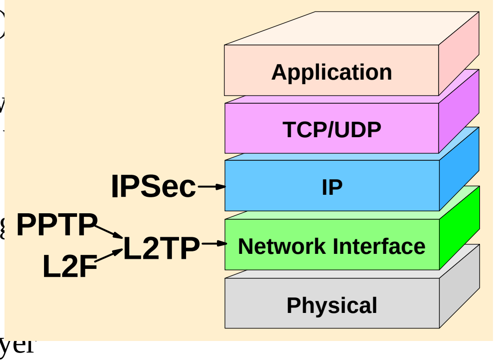

Figure 2. Positioning VPN Options

The Layer 3 Answer

IPSec is an IETF specification[3] that creates VPNs at Layer 3. As its name suggests, it provides the security lacking in L2TP. Since it is tied to IP, however, it can't natively carry other protocols. Of course, this is no problem if you're only sending IP data , but if other protocols are involved, you can use L2TP and IPSec in combination. In this arrangement, L2TP deals with the multi-protocol issues while IPSec handles security.

Opening the IPSec Envelope

IPSec is most appropriately thought of as a **framework** offering many choices rather than a monolithic standard that results in a set of look-alike VPN components. It is, in fact, this characteristic that gives rise to some of IPSec's greatest strengths (*e.g.*, flexibility) and its greatest weaknesses (*e.g.*, complexity).

IPSec essentially deals with three important VPN issues:

- Authentication (Are You Really You?)

[2] IETF Internet Draft: draft-ietf-pppext-l2tp-11.txt

[3] Security Architecture for the Internet Protocol (RFC 1825)

- Privacy (Just Between You and Me)
- Key management (But I Thought You Had the Key)

Are You Really You?

Authentication refers to the ability to know for certain that an entity is, in fact, who it claims to be. We do this in the physical world through informal means such as recognizing a person's appearance, voice, mannerisms, etc. These work well if you already know the person you're trying to identify, but in cases where you don't, then you can use more formal criteria involving credentials such as a drivers license, passport, or id card.. In the virtual world of cyberspace, such methods are impractical; however, digital counterparts derived from special applications of cryptography can do the job.

IPSec specifies an **Authentication Header** (AH)[4], which can be added to the original IP data packet to provide the following features:

- **Authentication —** Authentication is required when we need to know that the person (or thing) that we are communicating with is really who (or what) we think it is. For example, you may want to have your firewall authenticate packets coming into your network to ensure that they really came from your business partner and not a hacker intent on penetrating your defenses.
- **Message Integrity —** You might also like to know that the message that you sent is the same as the message that was received and that it has not been tampered with somewhere along the way. A saboteur could wreak havoc on your business by simply changing a few part numbers on an order you sent to a supplier. Instead of getting space heaters for your new Alaskan operation, you end up with a load of air conditioners. This might be good for a laugh the first time it happened, but on the 15th attempt, it wouldn't be nearly as funny.
- **Replay Protection** — In some cases a duplicate message is nothing more than a nuisance, but in the case of electronic commerce, the stakes are much higher. Let's say one of your customers sends an order for 100 hammers. A hacker saves a copy of this message and decides to re-send it to you 100 more times at carefully spaced intervals over the next few days. The folks in Sales might be headed for a celebration until they get the call from an irate customer who has a few choice words for the people that have him drowning in hammers. Replay protection detects, through the use of sequence numbers, that a packet has been seen before and can, therefore, be discarded.

Just Between You and Me ...

In some cases the AH features are sufficient to meet the business requirements, but if privacy is also an issue, then IPSec's **Encapsulating Security Payload** (ESP)[5] component should be used. The ESP function (indicated by the presence of an ESP header added to the IP packet [6]) calls for the original message contents to be encrypted before sending them out on the public network. The IPSec specification does not dictate precisely which cryptographic algorithm must be used but, instead, offers a set of choices such as DES, Triple DES, etc.

[4] IP Authentication Header (RFC 1826)

[5] IP Encapsulating Security Payload (RFC 1827)

But I Thought You Had the Key ...

Cryptography is based upon the assumption that both the sender and receiver know the predetermined keys (*i.e.,* a special string of bits) that allow them to encrypt and decrypt their communications. But how can both the sender and receiver determine such things as the exact encryption algorithms they will use for privacy and authentication, the encrypt/decrypt keys, the frequency with which these keys will be changed (to keep the hackers off-balance), and other IPSec options? What about the even more challenging problem of how to send these cryptographic details over a non-secured link in order to jump-start the entire process?

Of course you could simply determine all of this manually through “out of band” communications with the other party. Many of the initial IPSec implementations on the market are based on this arrangement. The advantages are that it is easier for vendors to build and it's more likely to interoperate. The disadvantage, however, is that it is more labor intensive for you to set up in the first place.

This is where the automated key management feature of IPSec come in. The **Internet Security Association and Key Management Protocol** (ISAKMP), like its higher level standard, IPSec, is more of a framework than a detailed specification -- in that it allows for various methods of establishing these details, which are known as **security associations** (SAs) .According to the specification, ISAKMP “provides a framework for authentication and key exchange but does not define them.” This allows ISAKMP to be used with a variety of key exchange protocols but, in fact, the industry has rallied behind only one - Oakley. As a result, you will often see the two names written together as **ISAKMP/Oakley** or in its newer, shortened form — **IKE** (Internet Key Exchange).[6]

The Envelope, Please ...

As discussed earlier from the security standpoint, sending a plain text message over the Internet is like sending a postcarc through the mail because the contents can be read by anyone along the delivery path. If a little more security is needed, you could seal the postcard in a special windowed envelope (*i.e.,* the kind that lets you see inside) with your company’s logo and return address on the outside. This way the recipient will have a greater degree of certainty that it really came from you (because presumably envelopes with your logo are not readily available to a would-be saboteur). Also, the recipient will be able to detect if the envelope has been opened and, potentially, tampered with. The cyberspace equivalent, shown in Figure 3, would be to use IPSec’s AH to authenticate the sender and ensure message integrity. The key difference in this analogy is that with the AH function, the window on the envelope exposes not only the address but the message contents as well.

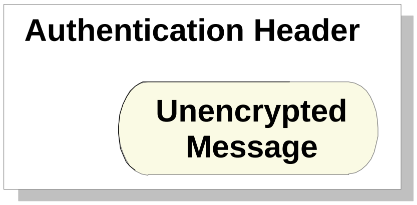

Figure 3. AH Envelope

[6] IETF Internet Draft: draft-ietf-ipsec-isakmp-oakley-08.txt

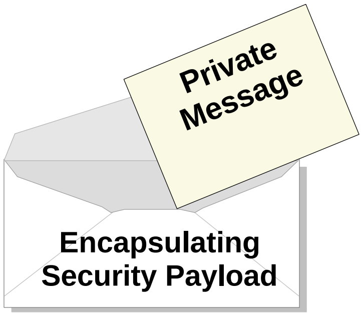

Figure 4. ESP Envelope

If that's not enough security, you could use a regular, non-windowed envelope to carry your message. This way the receiver could know the message came from you, know whether it has been tampered with, and know that no one else has read its contents since they have been obscured from view during delivery. As illustrated in Figure 4, IPSec's ESP performs an analogous function by encrypting the message. The ESP could also be used in combination with the AH features to provide additional security.

In some cases, though, even that is not enough. Let's say your business partner has a security policy that denies network entry to all unauthenticated traffic. Your message, however, must remain encrypted all the way to the receiver's system to ensure end-to-end privacy. You can satisfy both requirements by **nesting** one IPSec tunnel inside another. I other words, perform the AH and ESP processing on the origin message in order to make sure that only the intended receiver c read it and then wrap it in another AH layer designed to be read by your partner's firewall. This would be like putting your postcard in an opaque envelope and then putting it all in an oute transparent envelope. The mail clerk at the destination site removes the outer envelope and the recipient gets only the inner envelope containing the message. Figure 5 shows the real world equivalent of nested messages.

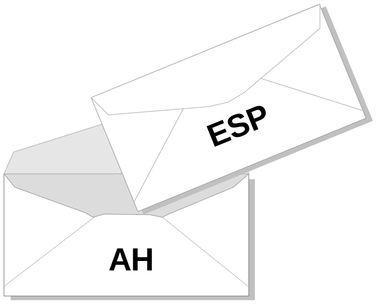

Figure 5. Nested Envelopes

And If That Weren't Enough ...

Let's say that you want to hide not only the contents of your message when it hits the Internet but also your IP address as well as the address of the recipient. You might want to do this for two reasons: A) because hackers can use such information to formulate their attacks or B) if you've used internal, non-registered IP addresses (*e.g.*, 10.xx.xx.xx), these can't flow on the Internet. The ESP, diagrammed in Figure 6, offers a **tunnel mode** which encrypts not only the message but also the IP header by ***encapsulating*** (a term often used synonymously with *tunneling*) the entire packet inside the ESP portion and building a new IP header containing different source and destination addresses (*e.g.*, the address of the firewall). If you don't need this level of protection, then you can use basic **transport mode,** resulting in lower overhead.

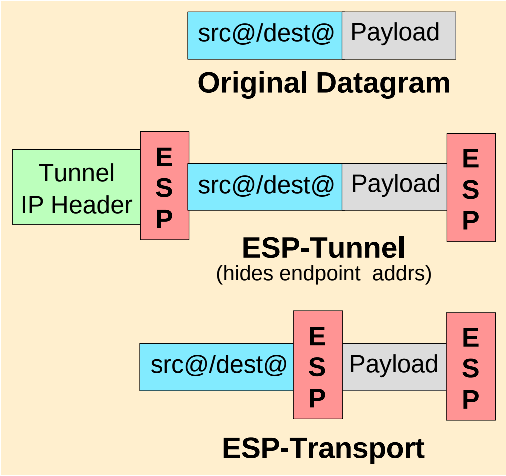

Figure 6. ESP Modes

AH also offers *transport* and *tunnel* modes, which have a similar effect, as shown in Figure 7. As with ESP tunnel mode, AH tunnel mode builds a new IP header and the AH authenticates the entire newly built packet. Since AH transport mode relies on the original IP header, it has lower overhead.

Stated simply, transport mode is intended primarily for host-to-host communications, whereas, tunnel mode is designed for situations where intermediate gateways (*e.g.*, firewalls) need to be involved in setting up or breaking dow the layers of the VPN.

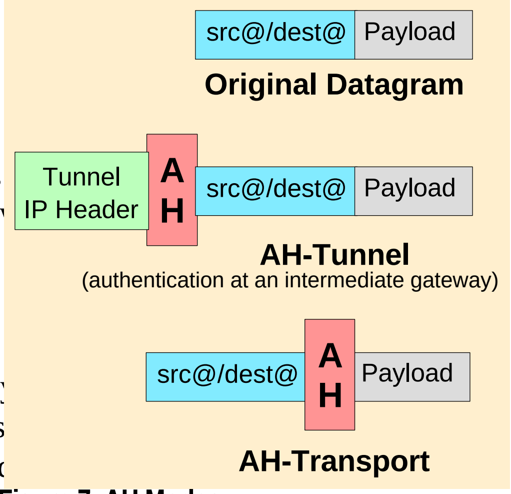

Figure 7. AH Modes

The Light at the End of the Tunnel

If this all sounds rather complicated, then you've obviously been paying attention. Setting up and maintaining VPNs is certainly not a trivial task. However, solutions do exist and there is reason to believe that the situation is getting better.

Some of the trickiest details with VPNs involve interoperability issues. Everyone claims to follow the standard but since the standard offers so many options, a multi-vendor turnkey installation is highly unlikely. Interoperability certification and testing from groups such as the International Computer Security Association (ICSA)[7], however, are a step in the right direction. ICSA offers both a general VPN certification and a more specific IPSec certification (which requires automatic key management using IKE) for products such as firewalls, routers, client systems, and server systems that can serve as VPN end points.

The bottom line, though, is that despite its inherent complexities, the potential cost savings (as compared to dedicated lines) and security benefits of VPN solutions are more than enough to justify a long, hard look at this important technology.

Reference

A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions, SG24-5201, Martin Murhammer, et al, IBM International Technical Support Organization, www.redbooks.ibm.com

[7] See www.icsa.net for more details.