Testing The Limits Of VPNs

Eric Krapf

IP VPNs have proven themselves—but only in proprietary implementations. Being "standard-compliant" isn't always enough.

In this sluggish corporate spending environment, Internet virtual private networks (VPNs) continue to attract attention as a way to reduce remote access costs for enterprise networks. For example, market researchers at Infonetics report that in 2Q01 the market for dedicated VPN hardware and software grew 19 percent quarter-over-quarter, to $535 million.

But while the number of implementations is clearly on the rise and VPN technology has become well understood, it also continues to be, in many respects, a work in progress. On the plus side, most of the noise about competing protocols has died away, leaving IPSec as the clear basis for VPNs going forward. "Two years ago, it was not as clear to customers which VPN protocol would prevail," said Greg Smith, director of product marketing at Check Point Software. "Today, if you look at what every leading vendor in the industry is doing, they're coalescing around IPSec/IKE [IPSecurity/Internet Key Exchange]."

IPSec seems to be able to deliver the security that enterprises demand—assuming, of course, it's implemented correctly and security policies are followed. But there are technical issues to work through, and a number of real-life problems have cropped up. And on the issue of multivendor interoperability, real trouble may be brewing.

Feeling Insecure About Security?

Security experts seem confident that IPSec VPNs, when implemented properly, can withstand attacks. "We have not seen any [successful] denial of service attacks or security attacks on VPNs using IPSec during its existence, which has been since 1999," said Chris King, security practice director for Greenwich Technology Partners. "I'm sure people have tried, but it's just pretty hard to crack public cryptography."

But if IPSec itself isn't vulnerable, corporate networks and end users certainly are, and VPNs give the bad guys a new way to make mischief. There's been plenty of concern about extending the network out to hundreds or thousands of individual users—each with an always-on connection to the Internet. That means each of those individuals has to take steps to ensure that their connection is kept secure at all times.

Matt Baker, senior network engineer for Intel Online Services, maintains that network managers must be equally vigilant about site-to-site (also called LAN-to-LAN) VPNs. He notes that, while network managers may not be able to control individual users accessing via remote client software, they can impose multiple layers of security more easily in the client-to-LAN than is feasible in LAN-to-LAN.

For example, tunnels from individual clients usually require two levels of access control— the IPSec/IKE routine, and also usernames/passwords that the individual must enter each time the tunnel is established. By contrast, LAN-to-LAN tunnels don't necessarily require manual authentication by every user that wants to send data, each time he or she wants to use the tunnel. That means that once an intruder breaks into one LAN, he or she may have a clear path to the other. "Using LAN-to-LAN, you actually have less control over the client, the customer," Baker said.

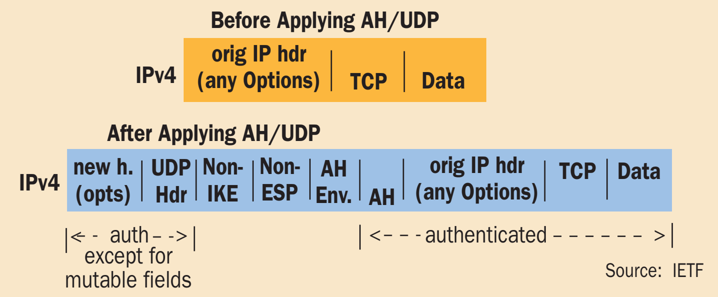
It's important, therefore, that the site-to-site VPN play a very specific, well-defined role. Matt Baker put it this way: "The best way to mitigate the risks of using a LAN-to-LAN tunnel is to squeeze it down to allow only what's needed. What are the networks at that site that need to pass over the tunnel, and what are the protocols that need to pass over it?"

NAT And IKEs—Yikes!

But getting your VPN implemented securely (also see *BCR*, March 2001, pp. 24–30), is just the beginning. There's also a not-so-simple matter of fitting IPSec with IP networks. Perhaps the most recently talked-about complication in VPN deployments is "NAT traversal"—implementing IPSec in an environment where user traffic goes through network address translation (NAT), which converts private IP addresses to public, routable addresses. The most common (though not the only) NAT scenario in the VPN world is a

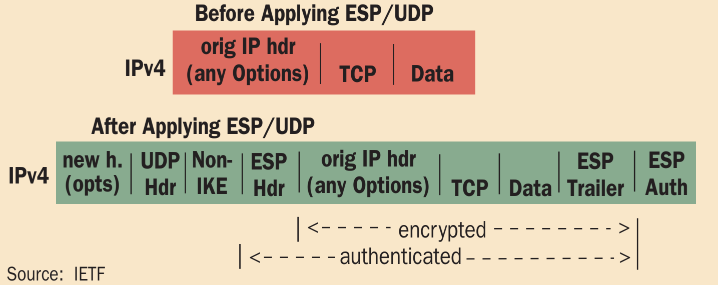
Eric Krapf is BCR's managing editor.

FIGURE 1a Tunnel Mode Authencation Header (AH) Encapsulation


Before Applying AH/UDP
IPv4
orig IP hdr (any Options)
TCP
Data
After Applying AH/UDP
IPv4
new h. (opts)
UDP Hdr
Non-IKE
Non-ESP
AH Env.
AH
orig IP hdr (any Options)
TCP
Data
|<- auth - -> | except for mutable fields
| <- - - authenticated - - - - - - >|

Source: IETF

FIGURE 1b Tunnel Mode Encapsulated Secure Payload (ESP) Encapsulation


Before Applying ESP/UDP
IPv4
orig IP hdr (any Options)
TCP
Data
After Applying ESP/UDP
IPv4
new h. (opts)
UDP Hdr
Non-IKE
ESP Hdr
orig IP hdr (any Options)
TCP
Data
ESP Trailer
ESP Auth
| <- - - - - encrypted - - - - - - - - >|
| <- - - - - authenticated - - - - - - - - - - >|

Source: IETF

telecommuter who tries to initiate a tunnel from behind a DSL or cable modem.

NAT is the classic example of how VPN implementations clash with the real world of IP networking, explained Intel's Matt Baker. "What NAT does is essentially what IPSec was designed to protect against. That is, tamper with traffic as it passes over a network." In other words, the receiving IPSec gateway interprets the act of address translation as an attack on the network and, therefore, drops the packet.

Vendors have adopted various means of dealing with NAT traversal, most often by encapsulating the IPSec packet in another protocol. The IETF addressed the NAT issue with a draft standard for encapsulation inside UDP (Figures 1a and 1b) earlier this year. Using this implementation, the address translation is performed on the wrapper IP address and the packet is then routed to its destination, where the encapsulation header is stripped off. The IPSec gateway at the destination sees only the original packet.

But that may not solve the problem. Heavy hitters such as Cisco, Nortel, Check Point and others support UDP encapsulation, but some also offer other schemes. Check Point, for example, has offered UDP encapsulation for more than a year, but recently came out with TCP encapsulation; Enterasys uses HTTPS, or SSL-secured HTTP.

Moreover, UDP may not be ideal for all NAT scenarios, according to Lori Sylvia, senior product marketing manager at Enterasys. While acknowledging that UDP is an effective way of getting around NAT for teleworkers on home broadband connections, Sylvia notes that there are other scenarios, mostly involving sales people, consultants or anyone else who travels to a client site and works off that company's LAN, where UDP doesn't solve the problem. "Corporate firewalls don't typically have UDP ports open," she explained, "and proxy servers also aren't meant to handle UDP protocol" (Figure 2).

Sylvia maintained that by encapsulating VPN traffic inside HTTPS, the visitor's traffic will conform to the host company's policy on secure Web traffic for its own users. "If a company feels comfortable allowing encrypted traffic to exit their network, there isn't going to be any issue over breaching a company's security policy,," Sylvia said. "If a company doesn't allow HTTPS, then we wouldn't be able to traverse, and rightly so, because we don't want to breach a company's security policy."

It also turns out that in large VPNs, UDP isn't always an effective way to encapsulate Internet Key Exchange (IKE) protocol traffic, which sets up the VPN connection. According to Mark Elliott, product manager at Check Point, if an enterprise has hundreds of thousands of users, each employing digital certificates, the validity of the digital certificates is typically checked against certificate revocation lists (CRLs). "If a CRL is large enough, [UDP] can cause a fragmentation and actually cause the IKE negotiations to fail," Elliott said.

Encapsulating the IKE packets in TCP creates a more stable connection than is possible with UDP, Elliott said: "TCP is a stream-oriented, reliably delivered transport mechanism, versus UDP, which is kind of like a letter; it's not reliable, things can arrive out of order and fragmentation can occur."

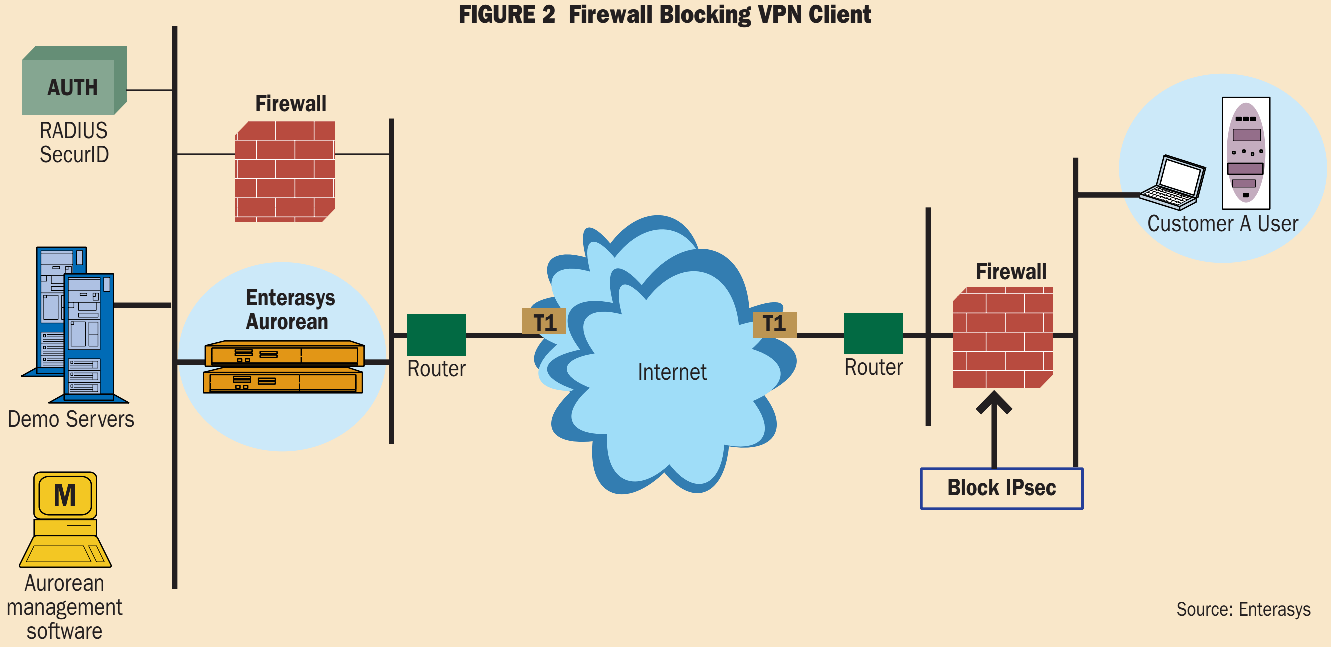
However, there's a tradeoff in using TCP as well, claimed Mike Ehlers, product line manager at NetScreen: "Basically, you're wrapping TCP within TCP, which adds way too much overhead to the overall connection end to end."

A Matter Of Philosophy

Issues like NAT traversal go beyond technical arguments over which protocol is best suited for which jobs. Like so many things in the security arena, the differing approaches of the vendors—and the position eventually adopted by users—makes a statement about what security means to that company. As Woody Weaver, director of professional services for Callisma consultancy, puts it: "It really boils down to the underlying security philosophy, more than anything else."

It seems to come down to deciding what to police: Network *traffic* or network *users*. While these are not mutually exclusive, Enterasys's position is that a visiting user on a corporate LAN is obeying the security policy if he or she behaves acceptably, i.e., sends only approved traffic.

FIGURE 2 Firewall Blocking VPN Client



Source: Enterasys

Others are more absolute, arguing that security arrangements should be spelled out between the individuals involved. "We don't believe you should just try to glom onto an existing allowed protocol," said Check Point's Mark Elliott. "You should really require an explicit 'allow' through the firewall."

Standard-Compliant vs. Interoperable

NAT traversal also illustrates another major issue in VPNs today—interoperability—which has implications even for enterprises that have or plan to deploy proprietary, single-vendor solutions: The more widely deployed VPNs become, the more likely it becomes that, whether as a result of a merger, acquisition or some other business deal, companies are going have to interoperate their VPN systems.

In addition, any form of extranet VPN—using the Internet to slash the cost of doing business with other enterprises—can't succeed without interoperability.

In the case of a merger, one of the parties is probably going to have to get rid of their existing gear. Without full interoperability, "we're going to get more and more proprietary implementations out there, and eventually someone's going to get bit," said Joel Snyder, senior partner of Opus One consultancy.

So where do we stand today? Not surprisingly, the vendors all say they're committed to standards, but they're also committed to putting their own spin on their product—as in the case of NAT traversal—based on things they say their customers want.

Some consultants are optimistic about interoperability for site-to-site VPNs, and they also believe that client-to-LAN interoperability is coming along. "If you go to Nortel, Nokia, NetScreen, Check Point, Lucent, Avaya, you're going to get a solution that is not proprietary, basically interoperable for your site-to-site VPN. In addition, you'll get a client which is more or less mostly standardized, maybe a little proprietary edge for authentication or address assignment, something like that," said Joel Snyder.

However, the experience of the world's largest extranet VPN effort—ANX—suggests that skepticism is warranted when it comes to claims of interoperability. ANX began as an auto industry effort and has expanded to 900 member companies worldwide, 111 of whom represent the top companies in the automotive supply chain. To participate in the ANX network, members must use equipment certified to interoperate sufficiently with the infrastructure deployed by ANX and its approved service providers—Ameritech, AT&T, Bell Canada, Equant, Ideal Technology Solutions and WorldCom.

However, ANXeBusiness, which owns the ANX network, recently announced that the lack of interoperability will affect plans for its own services—-it will offer a managed VPN offering based on a single vendor platform (which hadn't been chosen as of early September). ANX officials say that the IPSec specs simply allow too much variation, even among "standards-compliant" implementations.

That's not an unheard-of problem in networking, but it's proved particularly frustrating for ANXeBusiness. "The differences in the standard today are pushing costs into companies that they don't want," explained Richard Stanbaugh, VP of strategic initiatives at ANXeBusiness.

Vendor’s efforts on interoperability have been “good, but not good enough”

“We’re getting good cooperation from the vendors, but, frankly, not good enough,” added ANXeBusiness CTO Erik Naugle. “There’s no good way of ensuring interoperability on an ongoing, going-forward basis, except to limit the pool of IPSec vendors used on the ANX network.” Moreover, he expects this situation to continue “in the near term and probably longer term.”

As one example, Naugle cited the way standard-compliant VPN gateways negotiate the re-establishment of tunnels after a failure. “If one vendor chooses one of the menu options and another vendor chooses another menu option, the way it handles errors and timeouts can be completely incompatible and tunnels are not re-established upon failure,” he said.

Further complicating the situation, according Naugle, is that “every vendor is coming out with new revisions to their software on at least a quarterly basis, and the permutations on regression testing are just daunting if you have a large number of vendors constantly iterating their product.”

ANX’s decision and the reasoning behind it doesn’t bode well for the notion that companies will be able to build their own extranet connections anytime soon. Indeed, it suggests that they’ll have to turn to service providers—like ANX.

Conclusion

None of the problems described above are likely to stop a VPN deployment in its tracks. Rather, as Matt Baker of Intel sums up the situation: “VPNs are great, they do a lot for a lot of different people, and they can really help reduce your costs for remote access. But they’re not a magic bullet, and they don’t come without cost.”□

Companies Mentioned In This Article

Ameritech (www.ameritech.com)
ANXeBusiness (www.anx.com)
AT&T (www.att.com)
Avaya (www.avaya.com)
Bell Canada (www.bell.ca)
Check Point Software (www.checkpoint.com)
Cisco (www.cisco.com)
Enterasys (www.enterasys.com)
Equant (www.equant.com)
Ideal Technology Solutions (www.itsusnow.com)
Intel Online Services (www.intel.com)
Lucent (www.lucent.com)
NetScreen (www.netscreen.com)
Nokia (www.nokia.com)
Nortel (www.nortelnetworks.com)
WorldCom (www.wcom.com)

wwwpackets