



- Getting Started
- ▶ [Technology Solutions](#)
- ▶ [Department Reports](#)
- ▶ [Research Center](#)
- ▶ [Sales & Marketing](#)
- ▶ [FAQs](#)
- ▶ [Site Map](#)
- ▶ [Staff](#)
- ▶ [Article Index](#)
- ▶ [Current Issue](#)

## Security

## WORKSHOP

# Why Can't IPsec and NAT Just Get Along?

November 27, 2000  
By Mike Fratto

### Gimme the Good Stuff

Now here is where things get interesting. Let's look at some cases in which IPsec and NAT fail. NAT and AH IPsec will fail because, by definition, NAT changes the IP addressing of the IP packet. Any change in the IP packet will be flagged as a violation by AH. Failure also occurs when there is a NAT function between the two IPsec endpoints that doesn't know how to handle IPsec traffic.

Likewise, ESP IPsec and NAT will fail, because in the case of transport mode, the port numbers are protected by ESP, and any change will be flagged as a violation.

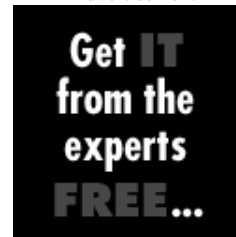
In tunnel mode ESP, the TCP/UDP headers are not visible and can't be used to translate between inside and outside. In this discussion, we are assuming that there is only one NAT device in the network. If there are more, they all need to be IPsec-aware to pass traffic properly. Static NAT and ESP IPsec will work just fine, because only the IP addresses are translated, regardless of upper-layer protocols.

Cisco Systems' Cisco 3060 and its VPN client support remote users through NAT by encapsulating the IP packet into UDP before hitting the network. Because the outer UDP and associated IP header aren't protected in any way, they pass through NAT devices of all kinds without a problem. The receiving Cisco 3060 must de-encapsulate the incoming packet and process it. This works only with the Cisco 3000 line.

There are other proposals in the IETF to standardize the encapsulation of IPsec in UDP, notably IPsec NAT-Traversal in the Network Working Group and RSIP (Realm-Specific IP) for end-to-end IPsec in the Network Address Translators Group. SSH Communications Security is making its NAT Traversal Toolkit available later this quarter.

### What's Left?

Advertisement



### Research and White Paper Locator

Within: Security

Network

**TechLibrary** Go!

- [Print Full Article](#)
- [Print This Page](#)
- [E-mail this URL](#)

### Other Workshops this issue

- ▶ [WAP: Untangling the Wireless Standard](#)
- ▶ [Buyer's Guide: Tape Autoloaders](#)

### Tools

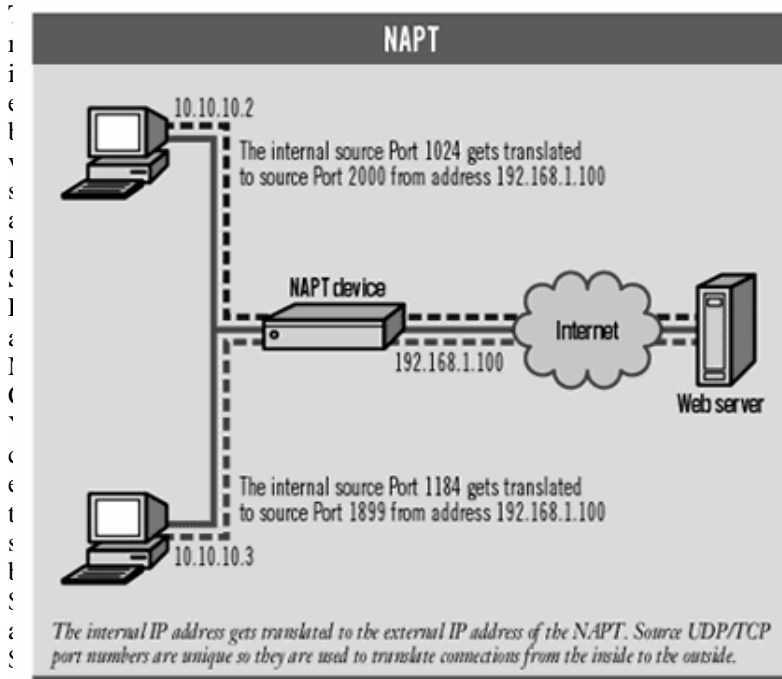
- ▶ [Attend Live Events](#)
- ▶ [Get IT Training](#)
- ▶ [Research Companies](#)
- ▶ [Find DSL Services](#)
- ▶ [Build Your Own RFP](#)
- ▶ [Get a Job](#)

RECEIVE 50% OFF AN ADDITIONAL INTEL® PENTIUM® III PROCESSOR 1 GHz WHEN YOU PURCHASE AN xSeries 330.

the n e-t

Netw the Je

So that leaves us with one situation: ESP IPsec with NAT. There are two ways that vendors are solving this problem. The simplest way, which allows only one IPsec VPN to pass through the NAT, is to associate a single workstation that is running IKE with all IPsec packets.



an SME NAT router.

Any IPsec packets that come into the NAT device are forwarded by default to the designated host. This is accomplished because the client starts the negotiation by sending data to the other end on Port 500. That process signals the NAT device to send all IPsec data back. Both ESP and AH are IP protocols and are assigned protocol Nos. 50 and 51, respectively. While not the most robust implementation, it does work for single installations. But what happens in the case where there are multiple workstations wanting to use IPsec?

In that case, you should get a product like Nexland's ISB2LAN or Asante Technologies' FriendlyNet 10/100 cable/DSL router, which supports multiple IPsec clients behind a NAT device. These more robust products run between \$150 and \$250, depending on the features.

To get NAT to work, we have to rely on the uniqueness of the source port number to translate between the private and public networks. Thus, we can negotiate IKE without any special process because IKE is a UDP protocol using Port 500.

To pass IPsec traffic between hosts, we need something equally unique, and we find that in our friend the SPI. Remember, each IPsec SA is identified by the SPI, the destination IP address and the protocol number. When IKE is negotiated during VPN setup, the SPIs are being exchanged, and the NAT device maps the pair of SPI numbers to the associated VPN endpoint behind the NAT (see "Translating IPsec").

The only SPI that needs to be mapped to an internal IP address is the incoming SPI selected by the IPsec client, because the NAT device needs to know where to send inbound traffic. Outbound traffic is passed without a problem, because the IPsec client's IP address will be changed by the

- ▶ Shop Our Advertisers
- ▶ Contact Our Advertisers



Get NWC

<< They're Free! >>

- Get the Magazine
- Get the Knowledge Alert Newsletter
- Get Our Weekly Newsletter
- Get the Security Newsletter
- Manage Your Existing Subscriptions

Spotlight

Special Report: **BrainShare Day 5**

Find out what Novell has in store for its flagship operating system, management tools and directory services with our special, daily report, direct from the show floor. Today, Novell goes to work for the state of Utah.

It's Coming...

**BEST OF SHOW**  
**NETWORLD+INTEROP**

Nominate Your Product Today!

Busin  
Awar



Tech  
Look  
opini  
the p  
softw  
tool,  
solut  
Tech  
onlin  
prod

Pow  
Find  
take  
perf  
next  
inter  
Com  
live l  
infor  
help  
best  
balar  
Rese  
today

Secu  
Subs  
Alert  
free,  
e-ma  
comj  
instr  
coun  
malic

- ▶ Dat
- ▶ Dig
- ▶ Conv
- ▶ Mo
- ▶ Apj
- ▶ Infi
- ▶ Ma
- ▶ Sec
- ▶ Ser

NAPT device.

There are some caveats, however. First, this scenario will work only when the IPsec client behind the NAPT device is initiating the IPsec VPN. If the IPsec gateway tries to initiate the connection, the NAPT device will block the negotiation, because it won't know where to send the UDP packets; it won't have a NAPT mapping. For the same reason, you cannot host a Web server behind a NAPT device without using port redirection, where all packets bound to a specific inbound port are by default sent to an internal IP address. Port redirection works only when preconfigured.

Second, for this to work, you will have to configure your IPsec gateway to negotiate IKE with the NAPT gateway at minimum or any IP address. ESP uses the SPI, destination IP address and protocol number to look up what SA an IPsec packet belongs to. Because the IPsec gateway knows the IPsec client only by the NAPT address, that is the address that will be used.

Finally, much of IKE authentication is still handled with a preshared secret, or password, which is associated with an IP address. Therefore, you have to tell the IPsec gateway to negotiate with the NAPT IP address. Because remote users often connect via dynamic IP addresses allocated from their ISPs, nearly all IPsec gateways can associate a shared secret with an address range.

If I knew, for example, that the NAPT device in translating IPsec would always come from an IP address on the 192.168.1.0 subnet, I would configure the IPsec gateway with one shared secret for the entire subnet. I would then have to configure each IPsec client behind that NAPT device with the same shared secret. As a result, this is really no different from how you go about typical IPsec remote access.

*Send your comments on this article to Mike Fratto at [mfratto@nwc.com](mailto:mfratto@nwc.com).*

PAGE: 1 | 2 | FIRST PAGE

[UnixWorld](#) | [Network Design Manual](#) | [Interactive Buyer's Guide](#) | [Tech Library](#) | [Real-World Labs](#) | [Learn IT](#) | [RFP Builder](#) | [Article Index](#) |

[Home](#) | [Technology Guides](#) | [Site Map](#) | [FAQ](#) | [Subscriptions](#) | [Contacts](#) | [Sales & Marketing](#) | [2001 Edit Calendar](#) |

**Network  
Computing**

[Bank Systems & Technology](#) | [CMPmetrics](#) | [eBusiness Expo](#) | [File Mine](#) | [InformationWeek](#) | [Insurance & Technology](#) |  
[InternetWeek](#) | [PC Expo](#) | [Planet IT](#) | [TechCalendar](#) | [TechEncyclopedia](#) | [TechLearning](#) | [TechReviews](#) |  
[TechWeb News](#) | [TechWeb Today](#) | [Wall Street & Technology](#) |



[Click Here!](#)

