



**ENCAPSULATING  
the EPS IN THE  
UDP**

**NETASQ**

*Secure Internet Connectivity*



## Problem covered by the document

An address in the middle of the VPN tunnel cannot be translated if IPSEC is used. In order to solve this problem for a tunnel between a VPN client and a NETASQ firewall the VPN's encrypted IP/ESP packets are encapsulated in UDP packets. This document provides all the information you need to understand encapsulation in a VPN and the incompatibilities between VPN and NAT (address translation) and it presents NETASQ's solution to the problem.

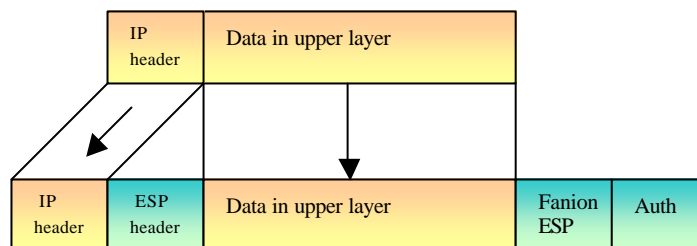
## Reminder about ESP encapsulation

In a VPN tunnel the data in IP packets transmitted between correspondents are encrypted and encapsulated in an ESP packet and then in a new IP packet. There are two encapsulation modes:

- **transport mode**, which keeps the original IP header. This mode is used when a tunnel has been established between two correspondents (the correspondents are the ends of the tunnel).



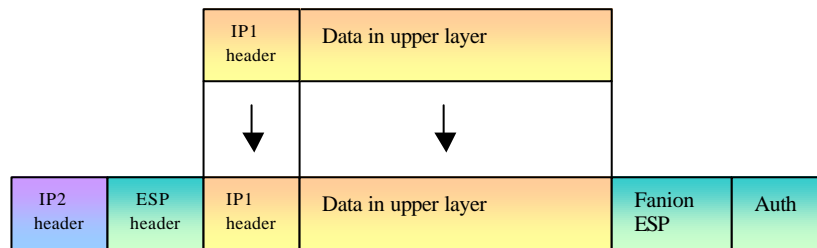
### *Encapsulation in the tunnel:*



- **tunnel mode**, which generates a new IP header using source and destination addresses (the two ends of the tunnel) instead of the correspondents' addresses



### *Encapsulation in the tunnel:*



**IP1** contains the IP addresses of the source and destinee machines

**IP2** contains the IP addresses of the VPN source and destinee passerelles

## Setting up a VPN tunnel

When a VPN tunnel is set up an SA (security association) is established for the two remote entities. It contains the parameters that enable them to set up security services between themselves. It also contains the AH or ESP security protocol which is used with security services, (confidentiality, integrity, authentication, protection against replay), the algorithms and encryption keys and the cutting option as well as the IPSEC protocol (tunnel or transport) and the SA's life expectancy. The following triplet identifies an SA:

- SPI index (Security Parameters Index)
- **Remote safety equipment address**
- Security protocol (AH or ESP)

A tunnel is linked to an SA. It is therefore directly connected with the IP addresses at both ends and the addresses used to identify an SA are their private addresses. (Note: the SA is re-established after a specified period of time).

When one end of a tunnel receives an IP packet with an ESP content it checks the corresponding SA for the packet. If the IP source address has been changed the entity can no longer determine the corresponding SA and the VPN tunnel cannot be fully established.

The VPN's path cannot be established if an address is translated on it because the source address at one end has been changed (private address to public address).

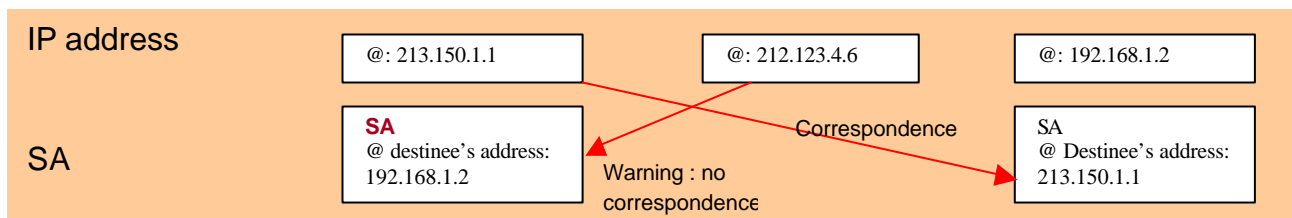
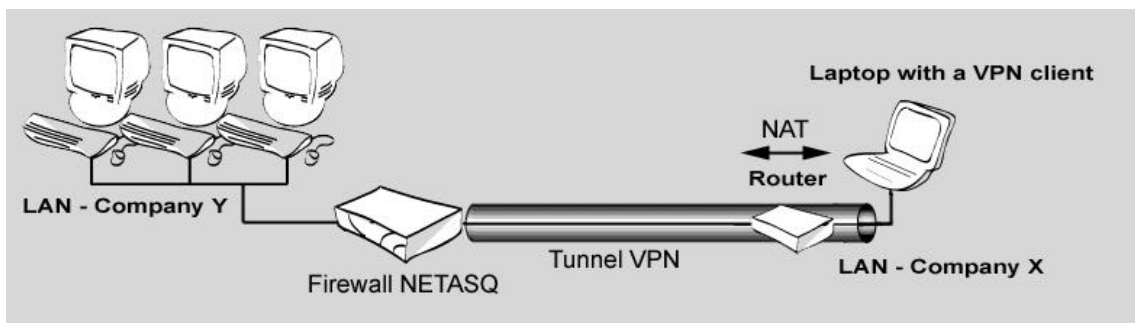
Entity can no longer determine the corresponding SA and the VPN tunnel cannot be fully established.

The VPN's path cannot be established if an address is translated on it because the source address at one end has been changed (private address to public address).

## Practical example

Company Y is a consultancy office in an organisation that carries out audits at clients' premises. One of the company's consultants has been sent to the client's premises at company X to analyse organisational malfunctions. The consultant must report daily to his superiors via the Internet. These reports must remain confidential even from company X's employees. The consultant therefore uses a remote extension which has a client VPN and must try to connect to his own company's LAN through a VPN tunnel.

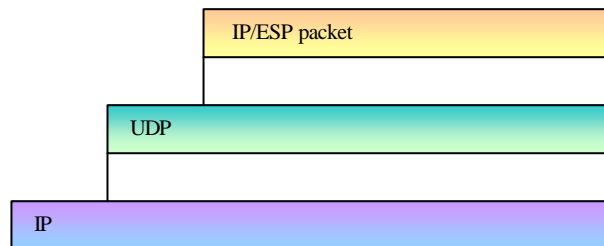
Unfortunately company X's router (or firewall) translates the address. The private address of the mobile extension sent to company Y's VPN gateway (Netasq Firewall) in order to set up the SA has been translated into a public address which does not match the one specifying the SA. The tunnel cannot be established and the consultant cannot contact his company's network via the VPN.



## Version 3.5 solution: supplementary UDP encapsulation

IP/ESP packets are encapsulated in the UDP in order to authorize the translation of addresses when using a VPN. **This option must be activated in the client's VPN.**

### Encapsulation detail



The IP address used to identify the SA is the one on the IP/ESP packet.

The source address on the VPN path can be changed easily because the VPN gateway will not check it to identify the SA. Data will be de-encapsulated as far as the IP/ESP packet at the VPN gateway, which will then compare the packet address with the SA's IP address (this time the two will correspond).

UDP is preferable to TCP as it adds less overheads and the encapsulated layers will manage the retransmission of packets if necessary.

### Limit

ESP encapsulation in the UDP is only tolerated for gateway/mobile client and not for gateway/gateway.