IPSec

Protocolli per sicurezza a livello di rete, garantisce autenticazione, integrità e riservatezza dei pacchetti IP. Due modalità:

trasporto header e trailer IPSec aggiunti al payload del datagramma IP, intestazioni IP non protette;

tunnel all'intero datagramma IP, che viene incapsulato in un altro datagramma.

In particolare, la specifica ESP (Encapsulating Security Payload) prevede:

- aggiunta di un trailer di padding al payload;
- cifratura di payload e trailer;
- aggiunta di intestazione ESP, con parametri per il cifrario e numero di sequenza (per contrastare attacchi di replay);
- aggiunta di MAC in fondo, calcolato su header, payload e trailer;
- aggiunta delle intestazioni IP, con numero di protocollo 50.

VPN

IPSec permette di realizzare reti private virtuali sull'Internet pubblica. I datagrammi da spedire ad altri host nella stessa VPN ma su reti locali diverse sono trasferiti con IPSec in modalità tunnel: