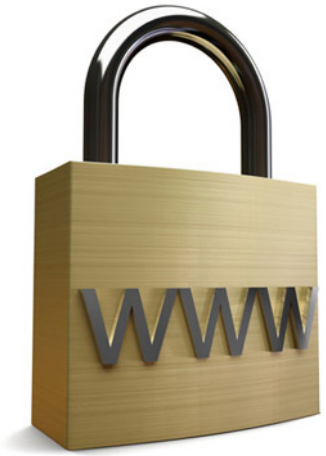
Inatel
Instituto Nacional de Telecomunicações

www.inatel.br

Segurança em Redes de Telecomunicações

SEGURANÇA DE REDES

Prof. Dr. Guilherme Pedro Aquino
guilhermeaquino@inatel.br

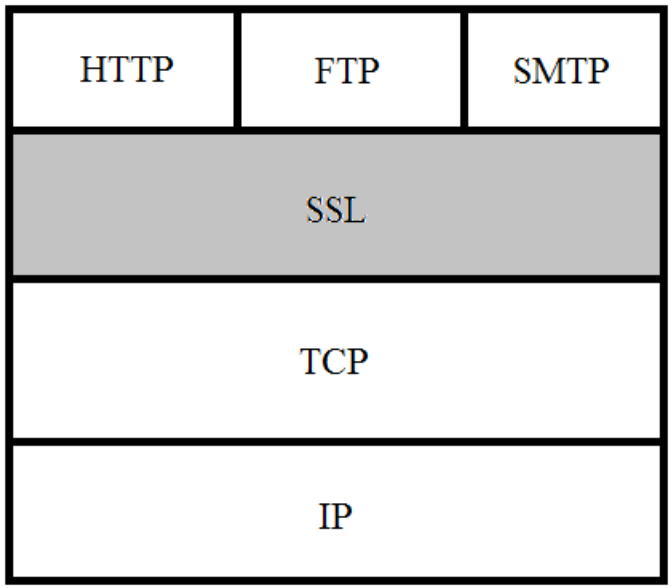


INATEL
Av. João de Camargo, 510
Santa Rita do Sapucai - MG
Tel: (35) 3471-9200

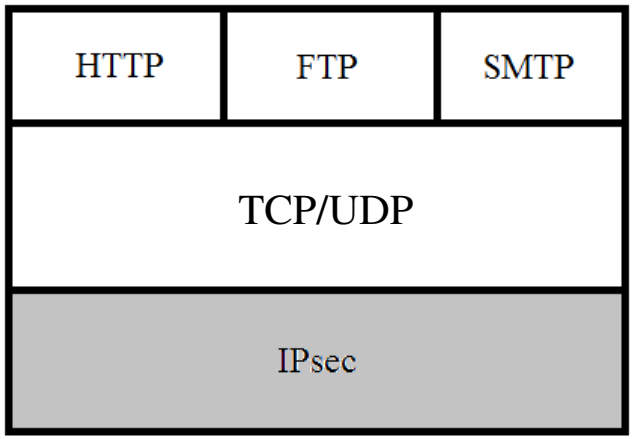
- Segurança nas diversas camadas do modelo TCP/IP

Segurança na Web

- SSL/TLS – Secure Socket Layer / Transport Layer Security.
- IPsec – Segurança na camada de Rede (Segurança IP).



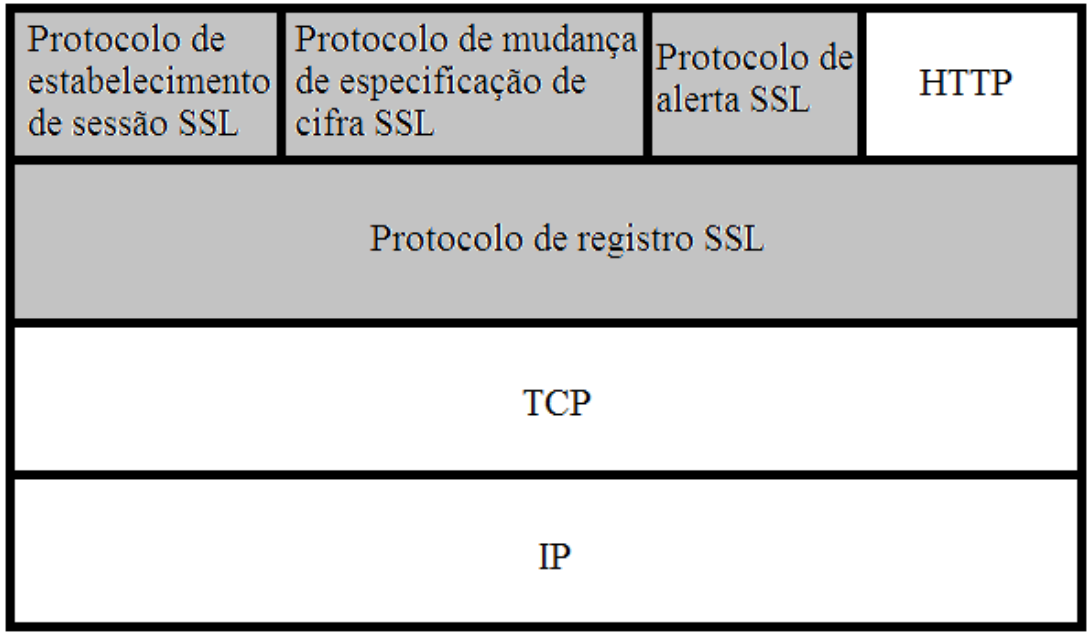
Nível de transporte



Nível de rede

SSL – Secure Socket Layer

- O SSL foi projetado para utilizar TCP e oferecer um serviço seguro confiável de ponta a ponta. O SSL não é um protocolo isolado, mas duas camadas de protocolos.



Arquitetura do Protocolo

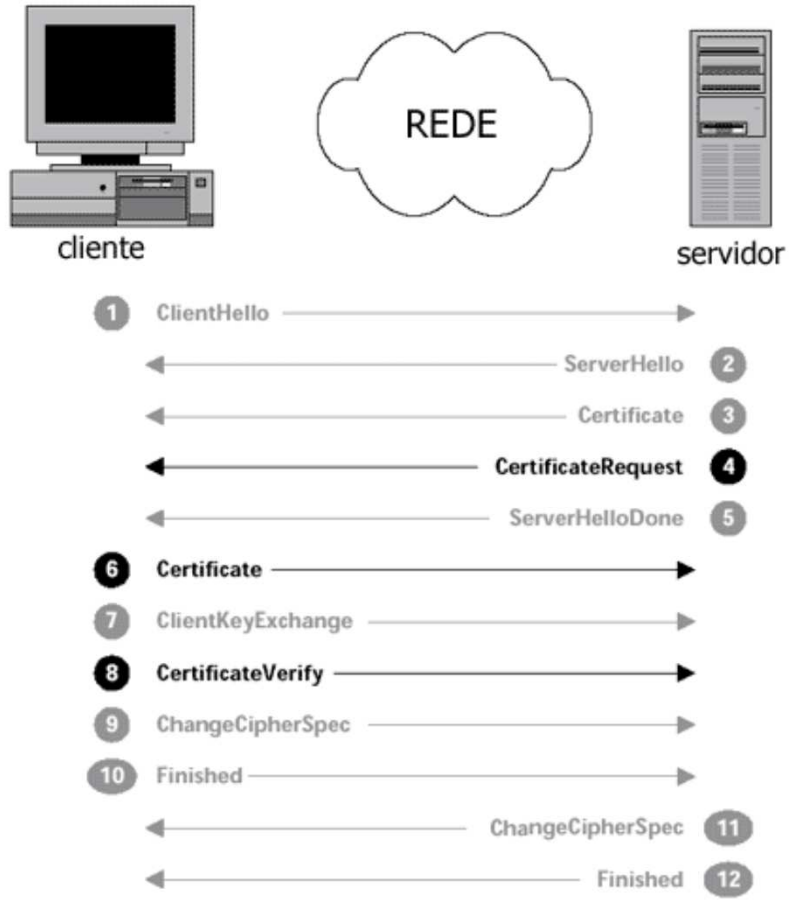
- O objetivo principal do protocolo TLS é oferecer privacidade e integridade dos dados em uma conexão entre duas aplicações.

- A conexão é privada. Criptografia simétrica é usada para encriptar os dados (DES, RC4, 3DES, etc). As chaves usadas na criptografia simétrica são secretas e únicas para cada conexão, geradas por negociação durante a etapa de handshake.

- O protocolo TLS e SSL combinam as criptografias simétrica e assimétrica, para contornar o problema do segredo pré-estabelecido da simétrica e o alto gasto computacional da assimétrica.

Fluxo de mensagens SSL

- Procedimento de autenticação de cliente e servidor



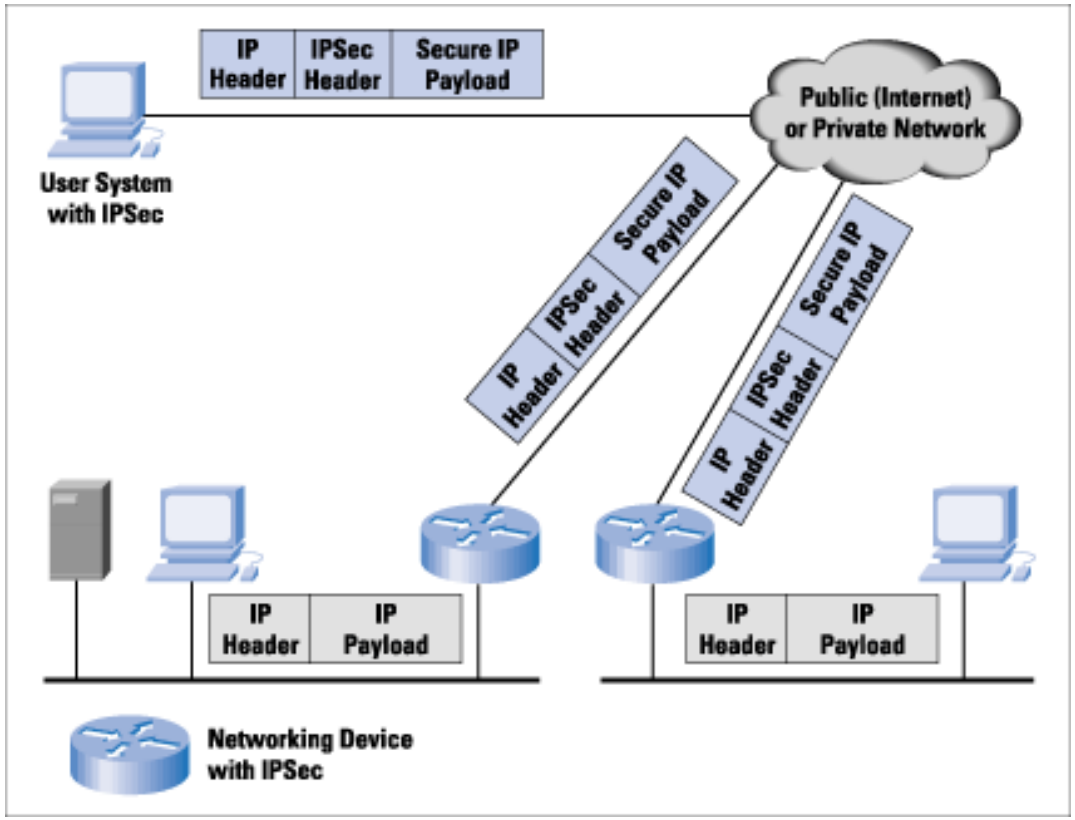
IPSec – IP Seguro

- O IPSec compreende três áreas funcionais:
  - Autenticação.
  - Confidencialidade.
  - Gerenciamento de Chaves.

- Aplicações do IPSec:
  - Conectividade segura do escritório pela Internet (VPN – Virtual Private Network).
  - Acesso remoto seguro pela Internet.
  - Estabelecimento de conectividade de extranet e intranet com parceiros, redes cooperativas.
  - Aprimoramento da segurança do *e-commerce*.

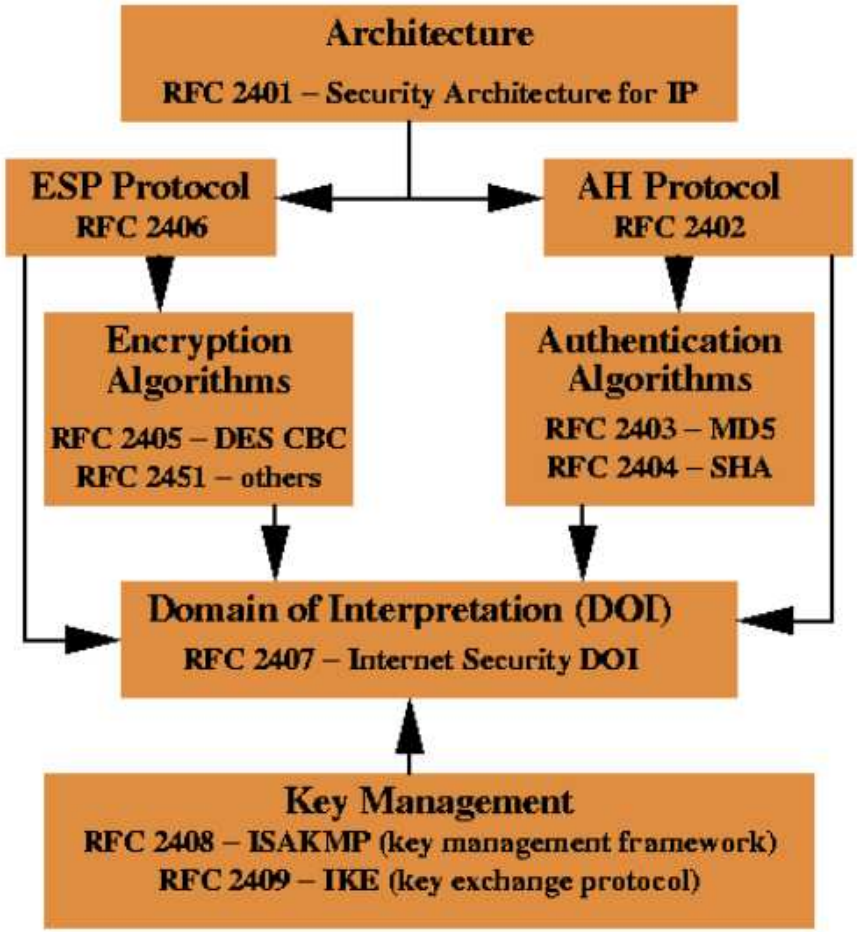
Estrutura IPSec

- O IPSec está abaixo da camada de transporte (TCP/UDP) e por isso, é transparente às aplicações. Pode ser implementado:
  - Sistema do usuário.
  - Firewall
  - Roteador



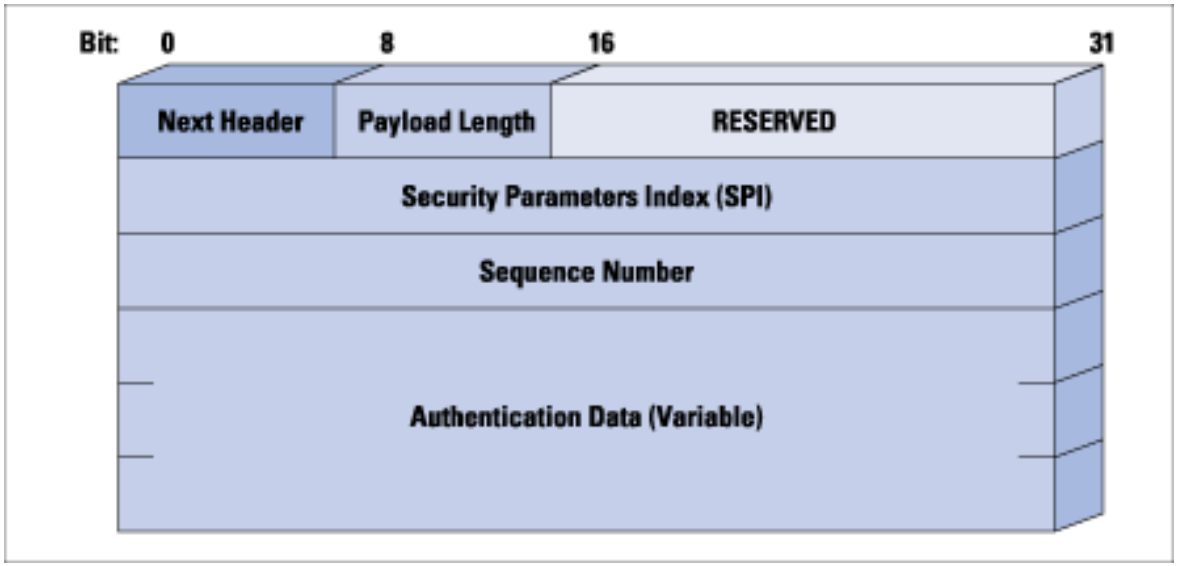
Documentação IPSec

- O IPSec é obrigatório no IPv6 e opcional no IPv4.



Cabeçalho de Autenticação – AH

- O cabeçalho de autenticação oferece suporte para integridade de dados e autenticação dos pacotes IP.

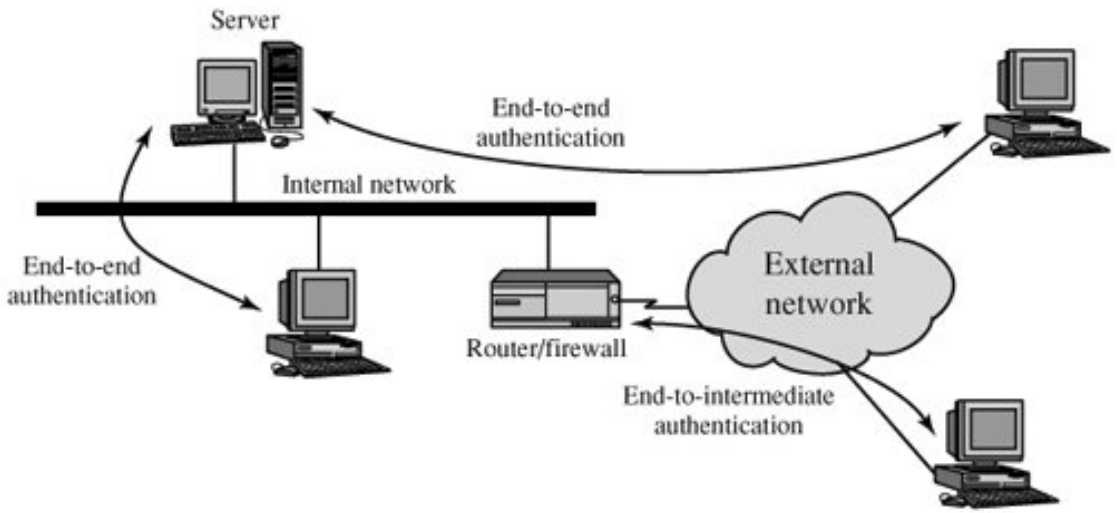


Verificação de Integridade

- O campo de Dados de Autenticação mantém um valor chamado de verificação de integridade (ICV – Integrity Check Value). O ICV é um código de autenticação de mensagem.
  - HMAC-MD5-96
  - HMAC-SHA-1-96
- HMAC (Hash-based Message Authentication Code)
- MD5 (Message Digest algorithm 5) – RFC 1321.
- SHA-1 (Secure Hash Algorithm)

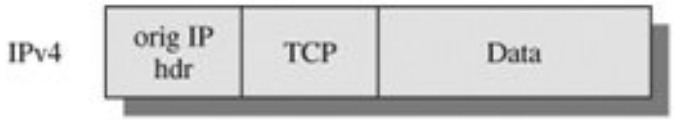
Modo Transporte e Modo Túnel - AH

- Modo Transporte.
  - A autenticação é fornecida diretamente entre um servidor e estações de trabalho.
- Modo Túnel.
  - A estação de trabalho remota autentica-se no firewall corporativo.

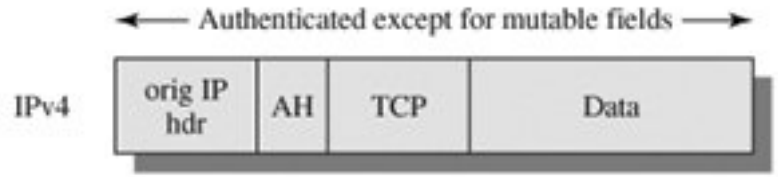


Modo Transporte e Modo Túnel - AH

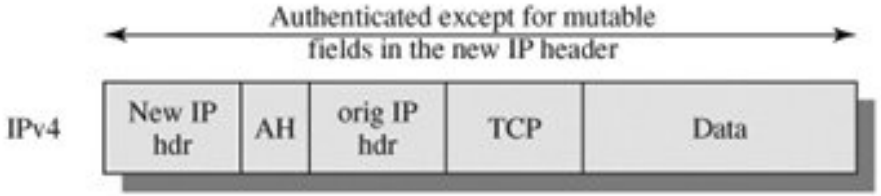
- Pacote IP original.



- Modo transporte.

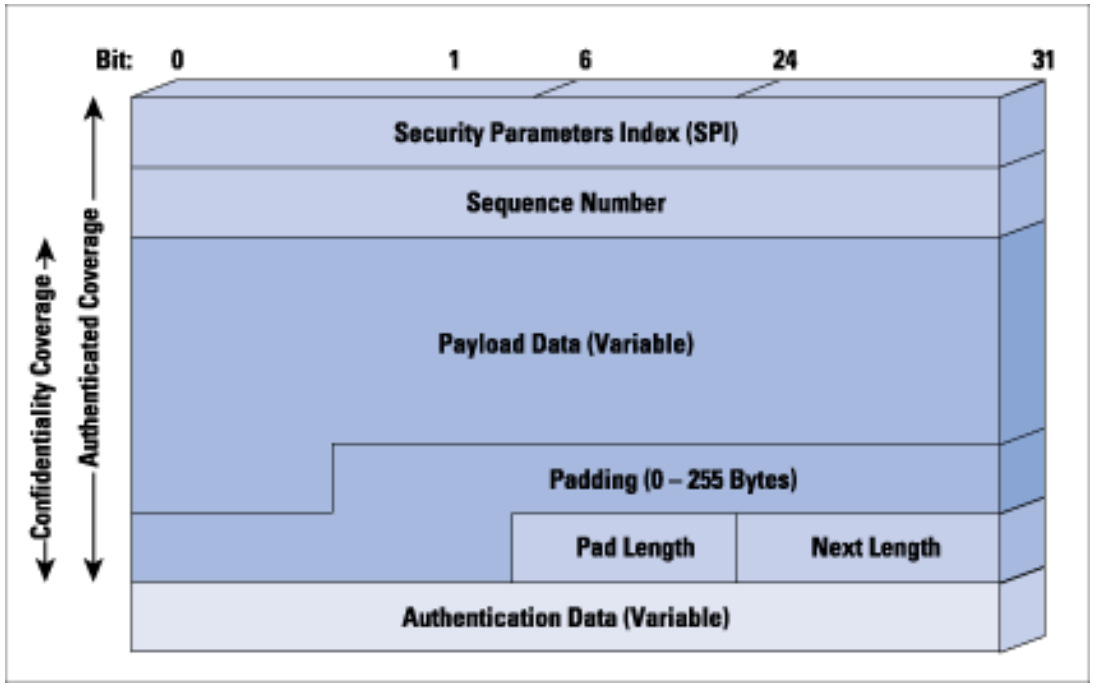


- Modo Túnel.



Encapsulamento de Segurança do Payload (ESP)

- O encapsulamento de segurança do payload (ESP) oferece serviços de confidencialidade de conteúdo da mensagem e a confidencialidade limitada de fluxo de tráfego. Como recurso opcional, o ESP também pode oferecer um serviço de autenticação.



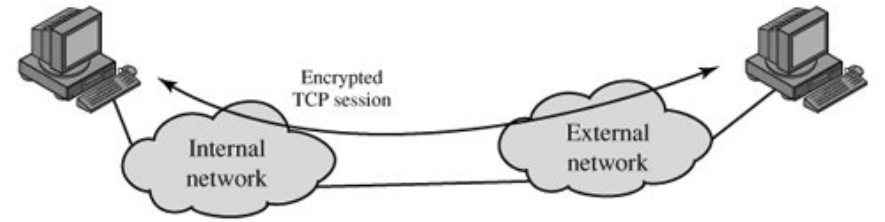
Algoritmos de Criptografia ESP

- Os campos Payload Data, Padding, Pad Length e Next Header são criptografados pelo ESP. Diversos algoritmos de criptografia são definidos no documento DOI (RFC 2407).

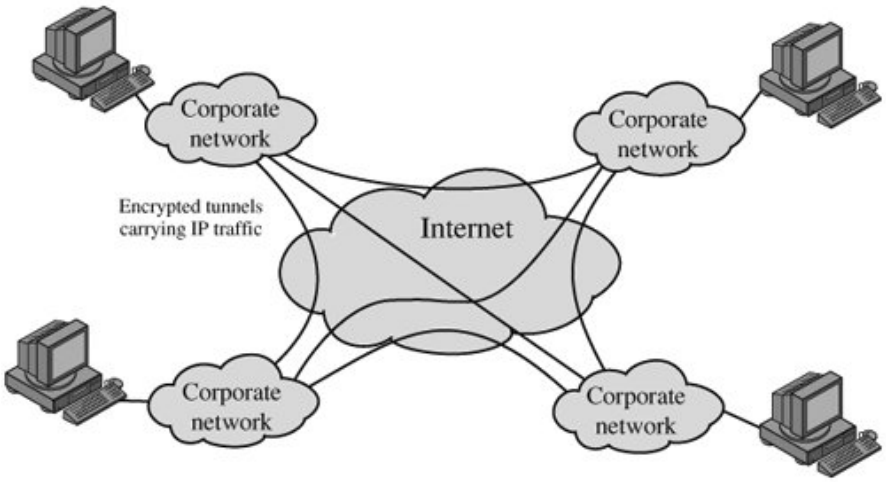
  - DES
  - Three-key Triple DES
  - RC5 (Rivest Cipher)
  - IDEA (International Data Encryption Algorithm)
  - Three-key triple IDEA
  - CAST (Carlisle Adams and Stafford Taveres)
  - Blowfish

Modo Transporte e Modo Túnel - ESP

- A figura abaixo mostra duas maneiras como o serviço ESP do IPSec pode ser utilizado. A criptografia pode ser obtida diretamente entre dois hosts. Ou pode ser usada para configurar uma rede privada virtual (VPN).



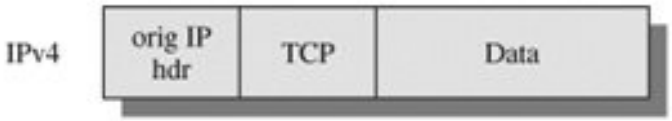
(a) Transport-level security



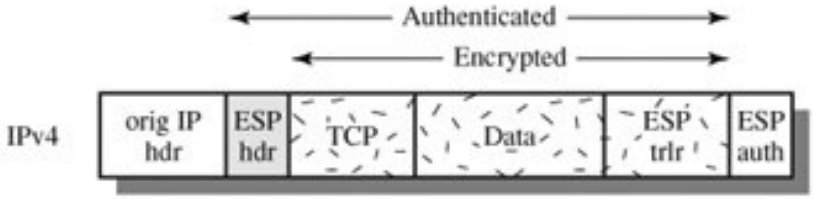
(b) A virtual private network via tunnel mode

Modo Transporte e Modo Túnel - ESP

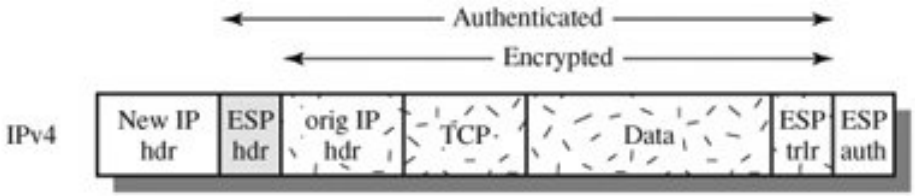
- Pacote IP original.



- Modo Transporte.



- Modo Túnel.



SSL versus IPsec

Característica	**SSL**	**IPSec**
Autenticação	usando tokens ou certificados digitais	usando tokens e certificados digitais
Criptografia	forte, mas variável pois depende do *browser*	forte e constante, definido na implementação
Complexidade de implementar	moderada	alta
Complexidade de uso	simples	moderada
Escalabilidade	alta	muito alta
Segurança total	moderada, pois cada dispositivo pode ser usado para criar regras	alta, pois define cada dispositivo e implementações
Camada OSI de atuação	7: *Application*	3: *Network*
Suporte a UDP	não	sim
Monitora sessão	sim	não
Cifra	dados	pacote
Autentica	sistema e usuário	pacote
PFS	sim	sim
Esconde IP internos	não	sim