IPSEC

O IPSEC, TAMBÉM CONHECIDO COMO O PROTOCOLO INTERNET SECURITY OU IP SECURITY, DEFINE A ARQUITETURA DOS SERVIÇOS DE SEGURANÇA PARA TRÁFEGO DE REDE IP.

AUTHENTICATION HEADER (AH): AUTENTICA O REMETENTE E DESCOBRE QUAISQUER ALTERAÇÕES NOS DADOS DURANTE A TRANSMISSÃO.

ENCAPSULATING SECURITY PAYLOAD (ESP): ISSO NÃO APENAS REALIZA A AUTENTICAÇÃO DO REMETENTE, MAS TAMBÉM CRIPTOGRAFA OS DADOS QUE ESTÃO SENDO ENVIADOS.

O IKE (INTERNET KEY EXCHANGE): PROTOCOLO DEFINIDO PARA PERMITIR QUE OS HOSTS ESPECIFIQUEM QUAIS SERVIÇOS DEVEM SER INCORPORADOS NOS PACOTES, ALGORITMOS CRIPTOGRÁFICOS QUE SERÃO USADOS PARA FORNECER ESSES SERVIÇOS E UM MECANISMO PARA COMPARTILHAR AS CHAVES USADAS COM ESSES ALGORITMOS CRIPTOGRÁFICOS.

EXISTEM DOIS MODOS DE IPSEC:

TUNNEL MODE: ISSO LEVARÁ TODO O PACOTE IP PARA FORMAR UMA COMUNICAÇÃO SEGURA ENTRE DOIS LOCAIS OU GATEWAYS.

TRANSPORT MODE: ISSO ENCAPSULA SOMENTE A CARGA ÚTIL DO IP (NÃO O PACOTE IP INTEIRO COMO NO TUNNEL MODE) PARA GARANTIR UM CANAL SEGURO DE COMUNICAÇÃO.