IPSEC

IPSec és l’abreviatura de Internet Protocol security. És un conjunt de protocols amb la funció es assegurar les comunicacions sobre el Protocol de Internet (IP) autenticant i/o xifrant cada paquet IP en un conjunt de flux de dades. IPSec també inclou protocols per l’establiment de claus de xifratge.

PROTOCOLS IPSec

Els protocols de IPSec actuen a la capa 3 de xarxa del model OSI. Altres protocols de seguretat per Internet d’ús extens, com SSL, TLS i SSH operen de la capa de transport (capa 4 del model OSI) cap a dalt. Això fa que IPSec sigui més flexible, ja que pot ser utilitzat per protegir protocols de la capa 4, afegint TCP i UDP, els protocols de capa de transport més utilitzats.

Una avantatge important de IPSec davant SSL i altres mètodes que operen en capes superiors, es que per que una aplicació pugui utilitzar IPSec no hi ha de fer cap canvi, mentre que per utilitzar SSL i altres protocols de nivells superiors, les aplicacions tenen que modificar el seu codi.

IPSec constitueix de dos protocols

PROPOSITS DEL DISSENY

IPSec va ser projectat per proporcionar seguretat en mode transport (extrem a extrem) del tràfic de paquets, en el que els ordinadors dels extrems finals realitzen el procés de.

IPSec pot utilitzar-se per crear VPNs i aquest es el seu ús principal.