Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Ejercicio IPsec – PC portátil

Presentación

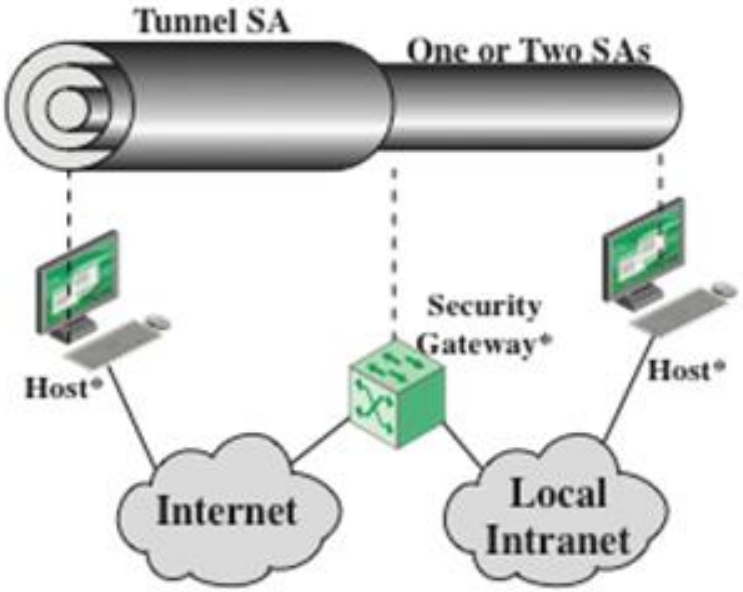
Daniel F. García

PC portátil se conecta a servidor con IPsec

Un Portátil se conecta a un Servidor de una corporación utilizando IPsec.
Para ello, el portátil establece dos Asociaciones de Seguridad (AS):

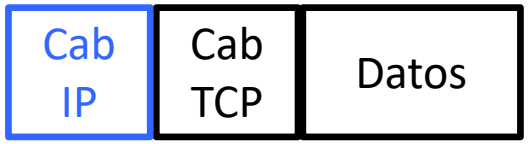
- La 1ª AS (interna) la establece con el servidor y
  usa el protocolo AH (Authentication Header) en modo transporte
- La 2ª AS (externa) la establece con el cortafuegos de frontera de la corporación y
  usa el protocolo ESP (Encapsulating Security Payload) en modo túnel sin autenticación

La combinación de Asociaciones de Seguridad se ilustra en la figura siguiente:



PC portátil se conecta a servidor con IPsec

Partiendo del paquete IP que se muestra en la figura siguiente, dibuja debajo el paquete intermedio generado por la 1ª AS y después el paquete final generado por la 1ª+2ª AS. Dibuja encima del paquete de la 1ª AS una flecha que cubra el ámbito de la autenticación y encima del paquete de la 2ª AS una flecha que cubra el ámbito del cifrado.



PC portátil se conecta a servidor con IPsec

¿Tiene sentido usar ESP con Autenticación, si ya se usa una AS de tipo AH para proporcionar un servicio de autenticación?