



Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Ejercicio IPsec – Dos Intranets

Presentación

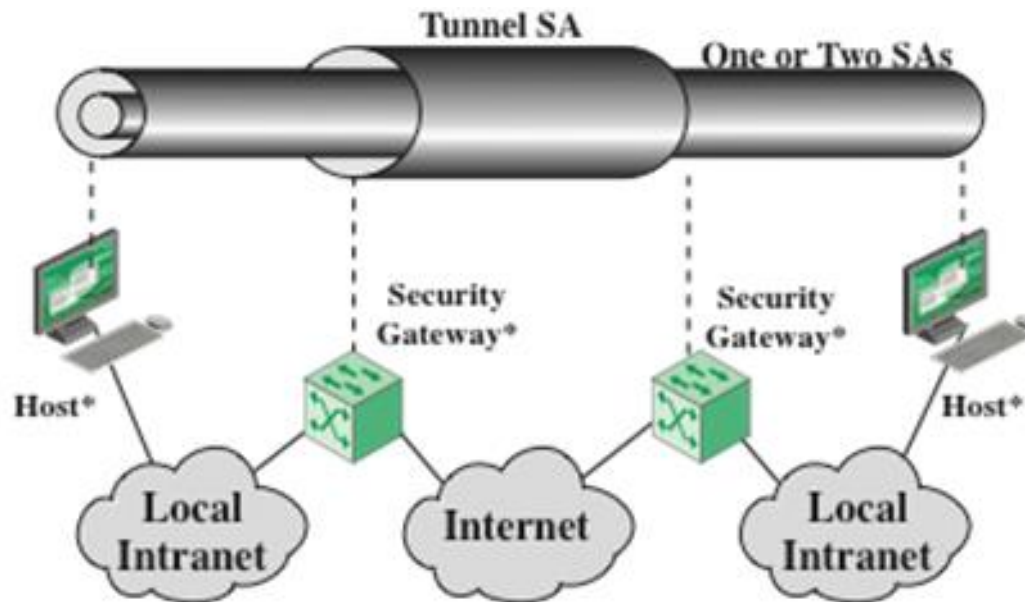
Daniel F. García

Conectar dos Hosts en dos Intranets con IPsec

Se desea proteger una comunicación entre dos hosts que están en dos Intranets geográficamente separadas y conectadas por Internet. Para conectarse de modo seguro usando IPsec se establecen tres asociaciones de seguridad (AS):

- La 1ª AS se establece entre los hosts y usa el protocolo AH en modo transporte.
- La 2ª AS se establece entre los hosts y usa el protocolo ESP en modo transporte sin autenticación.
- La 3ª AS se establece entre los Gateways y usa el protocolo ESP en modo túnel con autenticación.

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



Conectar dos Hosts en dos Intranets con IPsec

Partiendo del paquete IP que se muestra en la figura siguiente, dibuja debajo el paquete intermedio generado por la 1ª AS, luego por la 2ª AS, y finalmente por la 3ª AS. Debajo de cada paquete dibuja flechas que indiquen el ámbito de la autenticación y/o del cifrado, según corresponda.

AS1: AH-Tra
AS2: ESP-Tra Sin-A
AS3: ESP-Tun Con-A

