REDES PRIVADAS VIRTUALES VPN

Laboratorio de Redes de Computadores

Grado de Ingeniería Informática

Rosa Estriégana Valdehita

VPN

- Una *VPN* es una conexión virtual entre dos dispositivos que permite el envío de información de manera segura a través de un medio inseguro como lo es *Internet*.
- Proporcionan comunicaciones seguras con derechos de acceso específicos para los usuarios individuales.
- Mejoran la productividad al extender la red empresarial y sus aplicaciones.
- Reducen los costes de las comunicaciones y aumentan la flexibilidad.

Tipos de VPN

- **IPSec**
  Pros: Muy seguro, basado en estándares y muy adecuado para tráfico totalmente IP.
  Contras: Interoperatividad incompleta, costes de mantenimiento y falta de ubicuidad.

- **SSL**
  Pros: Bajos costes de mantenimiento (ya presente en los navegadores), no requiere mantenimiento en los clientes y buena interoperatividad.
  Contras: No soporta aplicaciones en tiempo real y no permite compartición de ficheros.

  Tabla comparativa entre ambas tecnologias
  http://www.thegreenbow.com/ipsecssl.html

VPN IPSec

- *IPSec (Internet Protocol Security)*. *IPSec* es un protocolo de capa 3 del modelo OSI que permite desarrollar *VPNs* brindando las siguientes ventajas:

- *Confidencialidad*
- *Integridad de la información*
- *Autenticación*

VPN IPSec

- ***Confidencialidad*** significa que la información enviada a través del *VPN* no podrá ser leída por un usuario o dispositivo tercero que no participe en la comunicación. La confidencialidad se logra a través de la implementación de técnicas de **cifrado** de datos. En *IPSec* podemos implementar cifrado de datos utilizando algoritmos simétricos tales como *3DES* y *AES*.
- ***Integridad de la información*** significa que la información enviada entre dos dispositivos en una *VPN* debe de llegar tal cual fue enviada por el emisor. En la práctica se logra a través de la implementación de técnicas de ***Hashing***. En *IPSec* podemos implementar *Hashing* utilizando algoritmos tales como *MD5*, *SHA-1* y *SHA-2*.
- **Autenticación** consiste en establecer mecanismos de seguridad para **validar la identidad** de los dispositivos envueltos en la transmisión de información a través de una *VPN*. En *IPSec* tenemos mecanismos de autenticación como son: (1) *Pre-share Key* y (2) *Digital Signature*.

VPN IPSec

- **IKE** “Internet Key Exchange” es un protocolo que define el método de intercambio de claves sobre IP en una primera fase de negociación segura.
- Está formado por una cabecera de autenticación, **AH** o Authentication Header, o una cabecera de autenticación más encriptación que se conoce como **ESP** o Encapsulating Security Payload

VPN IPSec

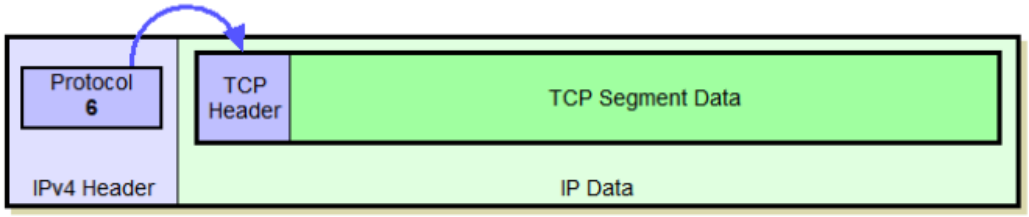
- IPSec ofrece dos modos de operación:

- **El modo transporte** cada segmento TCP junto con una cabecera (AH o ESP) viaja encapsulados en un datagrama entre el router fuente y el destino.
- **El modo túnel** En este modo, es el datagrama IP completo el que, junto con una cabecera (AH o ESP) viaja encapsulado en otro datagrama entre los routers fuente y destino.

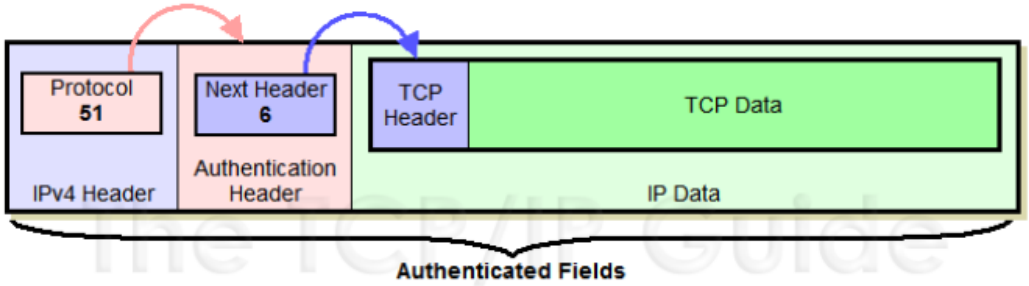
- En IPSec modo transporte la fuente y el destino de la comunicación llevan a cabo los controles de seguridad, por el contrario, en IPSec modo túnel la fuente y el destino no tienen la capacidad ni los recursos para llevar a cabo estos controles de seguridad en los paquetes.

- .

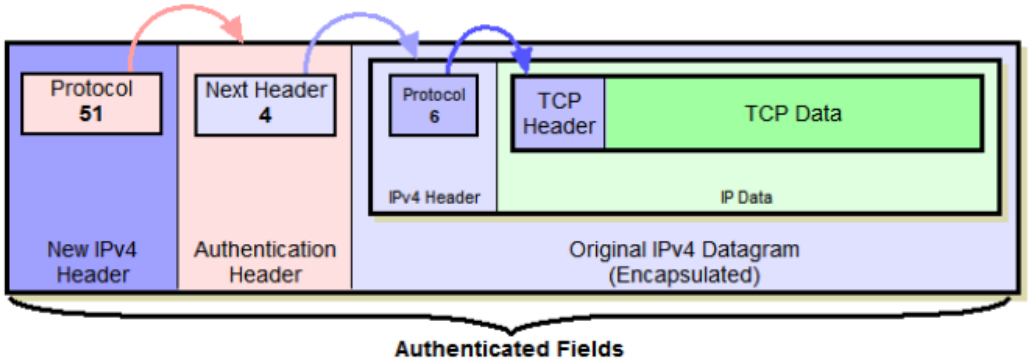
VPN IPSec



Original IPv4 Datagram Format

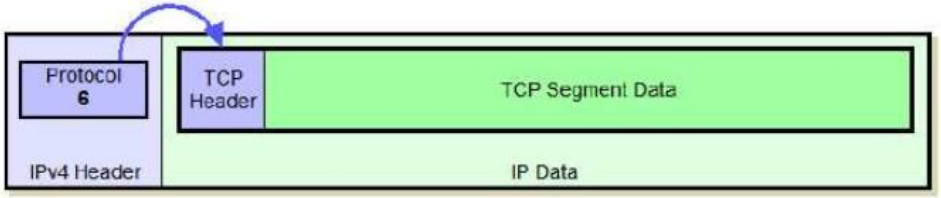


IPv4 AH Datagram Format - IPSec Transport Mode

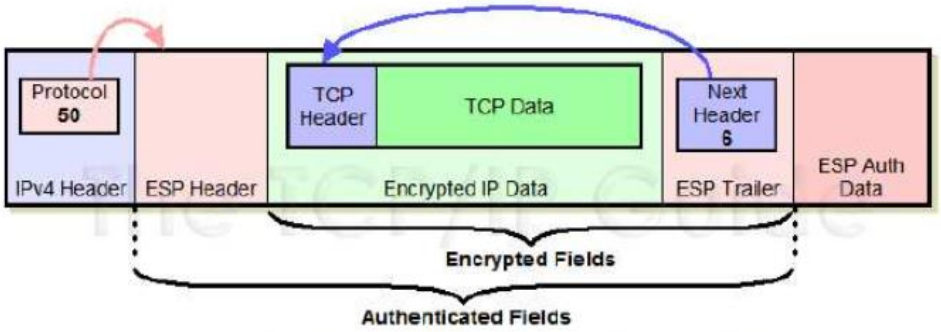


IPv4 AH Datagram Format - IPSec Tunnel Mode

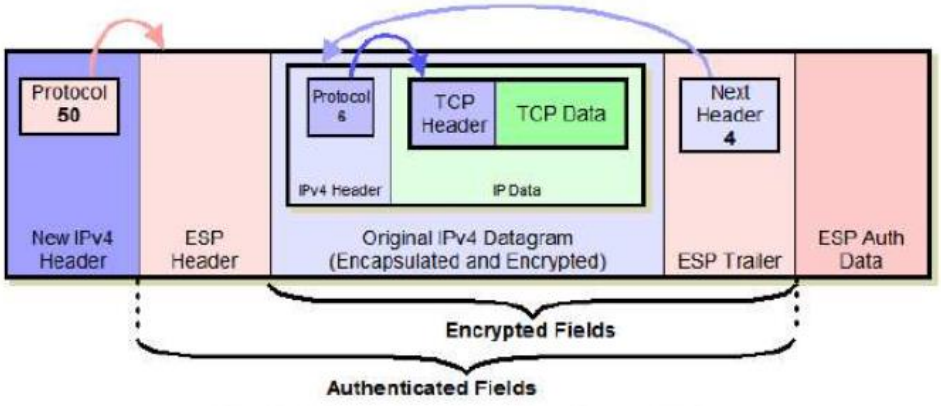
VPN IPSec



Original IPv4 Datagram Format

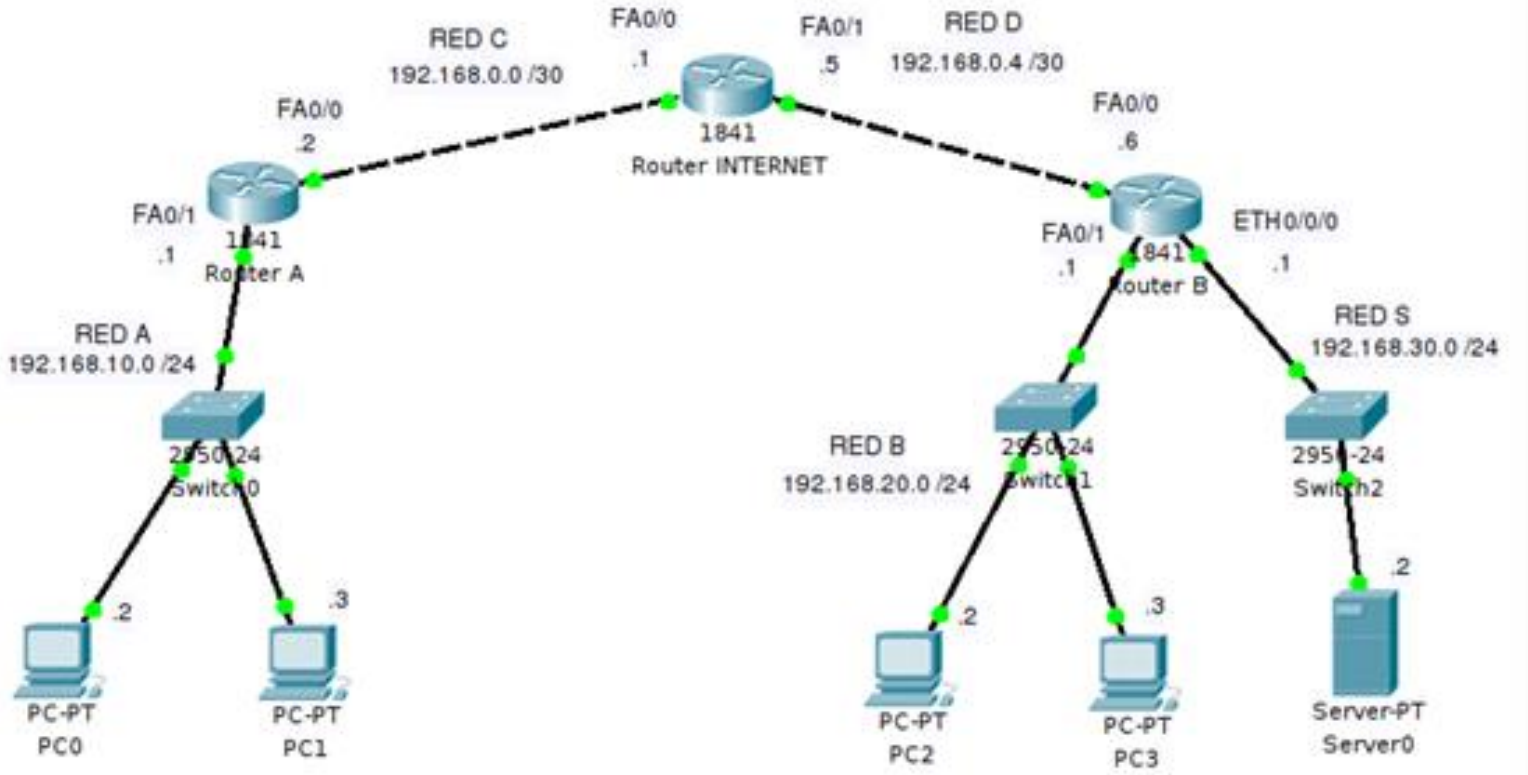


IPv4 ESP Datagram Format - IPSec Transport Mode



IPv4 ESP Datagram Format - IPSec Tunnel Mode

VPN IPSec



Crear una red privada virtual. Se debe permitir a los equipos de la RED A tener acceso a los equipos de la RED B y viceversa.
Para ello se utilizará encriptación y autenticación de datos entre las dos áreas utilizando **IPsec modo túnel**.

VPN IPSec

- Durante el establecimiento del tunel los 2 extremos negocian:
  - La autenticación
  - La encriptación
  - La gestión de claves

1. Definir Políticas de Seguridad

- *Router>**enable***
- *Router#**config term***
- *Router(config)#*
- *!--- Crear una ISAKMP policy. Definimos la prioridad en nuestro ejemplo 10.*
- *!--- Esta prioridad se utiliza para ordenar la aplicación de las políticas de encriptación cuando existen varias*
- *!--- Negociación del tunel.*
- *Router(config)#***crypto isakmp policy 10**
- *Router(config-isakmp)#***hash md5**
- *Router(config-isakmp)#***authentication pre-share**
- *Router(config-isakmp)#**exit***

2. Especificar clave compartida

- *!--- Especificar la clave compartida y la dirección remota del otro extremo del túnel.*
- *!--- Se identifica la clave (**vpnuser** en este caso) con la que se va a encriptar los datos*
- *Router(config)#***crypto isakmp key *vpnuser* address 192.168.0.6**

3. Crear Transform-set

- *!--- Crear un transform-set, por ejemplo con el nombre **myset**. El transform set define las políticas de seguridad que se aplican al tráfico que entra o sale de la interfaz.*
- *Router(config)#***crypto ipsec transform-set *myset* esp-des esp-md5-hmac**

4. *Crear el mapa criptográfico*

- *!--- Crear el mapa criptográfico por ejemplo con el nombre **mymap**.*
- *!--- Añadir una lista de control de acceso (ACL) para el otro extremo del tunel.*
- *Router(config)#***crypto map *mymap* 10 ipsec-isakmp**
- *Router(config-crypto-map)#***set peer 192.168.0.6**
- *Router(config-crypto-map)#***set transform-set *myset***
- *Router(config-crypto-map)#***match address 100**
- *Router(config-crypto-map)#***exit**

5. *Aplicar el mapa criptográfico*

- *!--- Aplicar el* mapa criptográfico *“crypto map”en la interfaz de salida.*
- *Router(config)#***interface fa0/0**
- *Router(config-if)#***crypto map *mymap***
- *Router(config-if)#***exit**

6. *Crear una ACL*

- *!--- Crear una ACL para el tráfico que va a ser encriptado. (de la RED A a la RED B)*
- *Router(config)#***access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255**
- *Router(config)#***exit**