Universidad de Alcalá

Departamento de Automática

REDES DE COMPUTADORES
Laboratorio

Práctica 5
Seguridad en redes IP

1ª Parte: Listas de control de acceso
2ª Parte: VPN (Virtual Private Network)

Grado en Ingeniería Informática
Curso 2018/19

1ª PARTE: LISTAS DE CONTROL DE ACCESO (ACCESS LIST)

Las listas de control de acceso (ACL) proporcionan un medio para filtrar los paquetes, permitiendo o denegando el tráfico de paquetes IP en las interfaces del router especificadas basándose en los criterios que se especifiquen en dicha lista de acceso.

Las ACL se escriben y se leen línea a línea de manera que cada línea es una regla para el router. Al final de las ACL va implícito un rechazo "deny all" o "deny any"

Para utilizar las ACL, el administrador del sistema debe configurar primero las ACL y luego aplicarlas a interfaces correspondientes.

Hay 3 tipos de ACL: estándar, ampliada y con nombre.

1. **Listas de acceso estándar (standard)**
   Son las más básicas, el rango va desde 1 a 99 y de 1300 a 1999.
   Solo se chequea la dirección fuente de todos los paquetes IP.

   Sintaxis de configuración:
   access-list access-list-number {permit | deny} source {source-mask}

   Aplicar la ACL a una interfaz
   ip access-group access-list-number {in | out}

2. **Listas de acceso extendidas (extended)**
   El rango va desde 100 a 199 y de 2000 a 2699.
   Se chequea tanto la dirección fuente como la dirección destino, y se puede especificar el protocolo (UDP, TCP, IP) y el puerto destino.

   Sintaxis de configuración:
   access-list *access-list-number* {permit | deny} *protocol* source {source-mask} destination {destination-mask} [eq destination-port]

   Aplicar la ACL a una interfaz
   ip access-group access-list-number {in | out}

3. **Listas de acceso con nombre (named)**
   Permite dar nombres en vez de números a las ACL estándar o extendidas

   Sintaxis de configuración:
   ip access-list {standard | extended} {name | number}

¿Dónde colocar la lista de acceso?

En líneas generales, las listas de acceso estándar se deben colocar cerca de destino y las listas de acceso extendidas se deben colocar cerca de la fuente.

¿Cuántas listas de acceso se puede utilizar?

Se puede tener una lista de acceso por protocolo, por dirección y por interfaz. No se puede tener dos listas de acceso a la dirección entrante de una interfaz. Sin embargo, se puede tener una lista de acceso de entrada y una de salida aplicada a una interfaz.

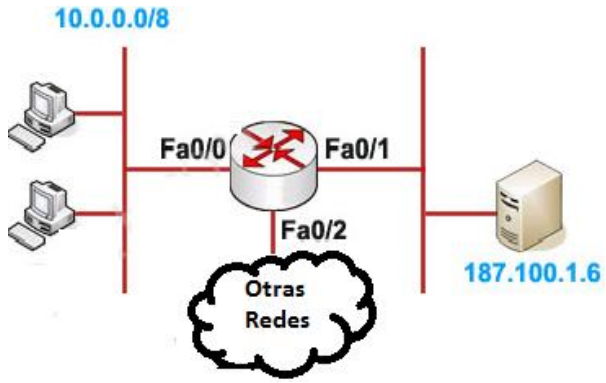
¿Cómo utilizar la máscara *wildcard* o máscara comodín?

Como ya hemos visto en varias ocasiones las máscaras se utilizan para especificar un host, red o parte de una red. En el caso de las listas de acceso se utilizan la denominada máscara *wildcard* o comodín donde en vez de ser 1's la parte referida a la red y 0's la parte referida a host es exactamente al revés.

Los ceros y unos en una máscara wildcard determinan si los bits correspondientes de la dirección IP deben ser revisados o ignorados para los propósitos de ACL.

Ejemplo de Lista de acceso estándar

Vamos a definir una lista de acceso estándar que permita solo a la red 10.0.0.0/8 acceder al servidor localizado en la interfaz Fa0/1.



Primer paso: Definir a quien se le permite el tráfico:

Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255

Siempre hay una prohibición implícita (deny) al resto de tráfico al final de la ACL y por eso no necesitamos añadir "deny" al resto de tráfico.

Nota: la máscara "0.255.255.255" es la "*wildcard mask*"

Segundo paso: Aplicar la ACL a la interfaz:

Router(config)#interface Fa0/1

Router(config-if)#ip access-group 1 out

La ACL 1 se aplica para que permita salir de la interfaz Fa0/1 solamente a los paquetes de 10.0.0.0 / 8 y deniegue el resto del tráfico.

Ejercicio 1: Listas de acceso estándar

OBJETIVO: Configurar una lista de control de acceso estándar para filtrar los paquetes que llegan al servidor **Server0** de manera que solo **PC0** de la RED A tenga el acceso permitido, denegando el acceso al resto; para ello hay que aplicar la lista de acceso en la interfaz del router cercana al destino.

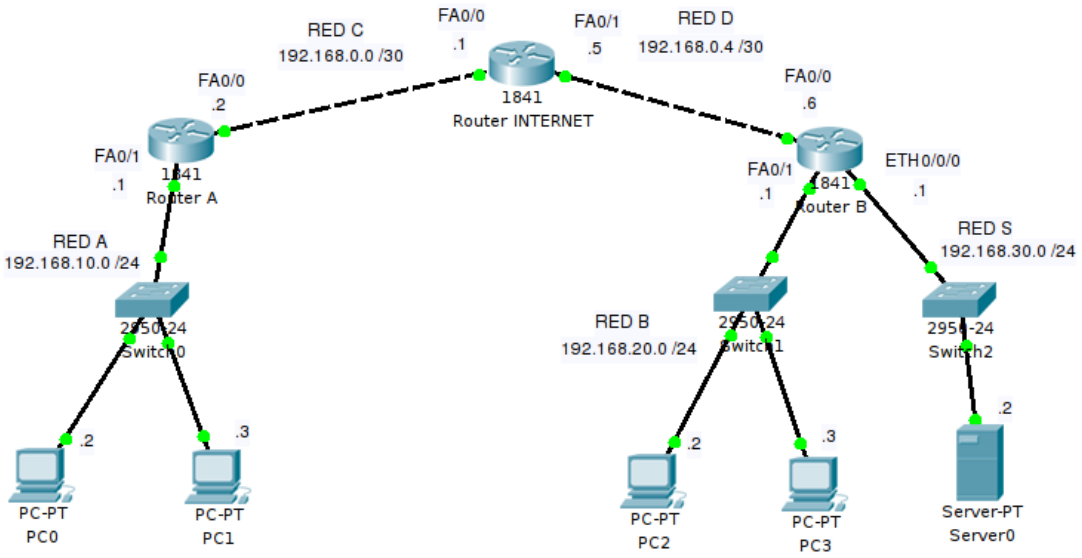


Figura 1

1.1 Crear la topología de la Figura 1

Utilizando el simulador Cisco Packet Tracer, cree la topología de red que se muestra en la **figura 1.** Guarde el fichero como **P5acl.pkt**

Nota: Necesitará añadir un módulo de conexiones al Router B.

Nota: El orden de las interfaces no tiene por qué ser como el de la figura, pero recuerde ser consecuente con las configuraciones.

1.2. Configuración de interfaces y tablas de enrutamiento

1. Configure los equipos siguiendo el esquema de direccionamiento de la figura: Asigne una dirección IP apropiada a cada uno de los PC's y a cada una de las interfaces de los routers.

2. Añada al esquema de Packet Tracer etiquetas con el número IP asignado y su máscara a cada interfaz y a cada equipo.

3. Configure las tablas de rutas convenientemente para que pueda existir conectividad entre todos los equipos. Asigne a las interfaces de los routers la primera dirección de cada red.

1.3. Verificación de la conectividad

4. Compruebe la conectividad entre todos los equipos.

   Para mantener la configuración de todos los equipos, aunque realicemos cambios posteriores, ejecute: Router#copy running-config startup-config

   Este esquema lo utilizaremos para la 2ª parte de la práctica por eso guarde una copia como **P5vpn.pkt**.

1.4 Configurar Lista de control de acceso estándar

1.4.1 Definir a quién se le permite el tráfico:

Router(config)#

1.4.2 Aplicar la ACL a la interfaz:

Router(config)#

Router(config-if)#

1.5 Compruebe haciendo ping la conectividad entre todos los equipos.

¿Podemos acceder al servidor desde todos los equipos?

1.6 Para permitir a toda la RED A y solo a la RED A, el acceso al servidor ¿Qué cambio deberíamos hacer en la ACL?

1.7 ¿Podemos aplicar esa ACL a otra interfaz del router B? ¿Por qué o por qué no? Razónelo

Ejercicio 2: Lista de acceso extendida

Siguiendo con el esquema de red de la **figura 1** se desea en esta ocasión crear una lista de acceso extendida que impida el tráfico FTP desde la RED A pero que permita cualquier otro tipo de tráfico.

Nota: FTP usa TCP en los puertos 20 y 21.

2.1 Eliminar la lista de acceso estándar creada en el ejercicio anterior

Router(config)# interface Fa0/1 (la interfaz correspondiente)

Router(config-if)# no ip access-group 1 out

2.2. Ejecute FTP al servidor desde uno de los PC's de la RED A

Desde PC0 o PC1 abra la pestaña Desktop, a continuación haga click en Command Prompt y escriba

>ftp 192.168.30.2 (o el nº ip que haya puesto en el servidor)

(username y password = cisco)

2.3 Definir el protocolo, qué fuente, qué destino y qué puerto son rechazados:

Completar:

Router(config)#access-list 101 ……..eq 21

Router(config)#access-list 101 ……eq 20

Router(config)#access-list 101 permit ip any any

2.4 Aplicar la ACL a la interfaz:

Router(config)#

Router(config-if)#

2.5 Explique ¿Por qué es necesario poner access-list 101 permit ip any any?

2.6 Comprobaciones:

Repita los pasos del apartado 2.2. Ejecute FTP al servidor desde uno de los PC's de la RED A

¿Qué sucede?

Compruebe si se puede hacer FTP al servidor desde un PC de la RED B.

¿Qué observa?

2ª PARTE: REDES PRIVADAS VIRTUALES (VPN)

Una red virtual privada, ***Virtual Private Network*** (**VPN**), permite una extensión segura de una red de área local (LAN) sobre una red pública o no controlada como es Internet, ofreciendo las funcionalidades de gestión y seguridad de una red privada; para ello es necesario establecer una conexión que ofrezca mecanismos de seguridad.

Un ejemplo habitual es conectar dos o más sucursales de una empresa utilizando Internet, o que un empleado acceda desde su casa a la red de datos de su empresa.

Las redes privadas virtuales se pueden configurar en la mayoría de los routers Cisco (800 a 7500). VPN puede ser implementado de múltiples formas y con diferentes niveles de seguridad.

Para entender mejor las redes VPN y comprender plenamente su potencial es necesario tener conocimientos de sistemas criptográficos y de algoritmos de cifrado.

Métodos de implementación de VPN
Hay dos formas principales para implementar una VPN:
- VPN basada en IPsec
- VPN basada en SSL

Ambos métodos ofrecen ventajas y desventajas.
Para implementar una VPN basada en **IPsec** hay que instalar el software de cliente en cada host o dispositivos que necesitan acceder a la VPN remota.
Por otro lado, las VPN **SSL** pueden establecer directamente la conexión entre dos máquinas sin necesidad de instalar ningún software cliente porque usa **TLS**, protocolo estándar de comunicación segura a nivel de transporte.

Proceso de diseño de una VPN

Para utilizar una VPN, por ejemplo, para una comunicación empresarial segura, es necesario diseñar un plan de implementación de VPN que debe tener en cuenta los siguientes aspectos:

1 . Identificar el tipo de VPN (SSL o IPsec) que necesita y cuáles son los sistemas informáticos o equipos de red que necesitan ser protegidos por una conexión VPN.

2 . Diseño de VPN: elegir el tipo de métodos de autenticación, filtrado y la política criptográfica.

3 . Prueba: es mejor tratar de probar el diseño en un entorno de prueba antes de implementar la VPN de la organización.

4 . Despliegue: una vez que se está satisfecho con el resultado de la prueba, se puede empezar a implementar la VPN según su diseño.

5 . Monitorización: seguimiento de la actividad de tráfico en los puntos finales de VPN y siempre teniendo en cuenta las advertencias de seguridad o actualizaciones.

IPsec

IPsec es un protocolo que está sobre la capa del protocolo de Internet (IP). El objetivo principal de IPsec es proporcionar seguridad en la comunicación, mientras que los datos pasan a través de la red pública Internet. Para establecer IPsec se necesita tener dispositivos compatibles IPsec.

IPsec utiliza la siguiente tecnología de seguridad.

- Criptografía de clave pública
- Intercambio de claves mediante Diffie-Hellman
- Cifrado de datos.
- Algoritmos resumen (*hashing*) que verifican la autenticidad e integridad de datos. Algunos algoritmos resumen utilizados son, por ejemplo, MD5 y SHA-1.

IPsec proporciona principalmente dos tipos de servicio: la autenticación y el cifrado de paquetes mediante el uso de AH y ESP.

AH (Autentication Header)- Proporciona integridad y autenticación, y evita el ataque por repetición. En cambio, AH no ofrece ningún servicio de cifrado.

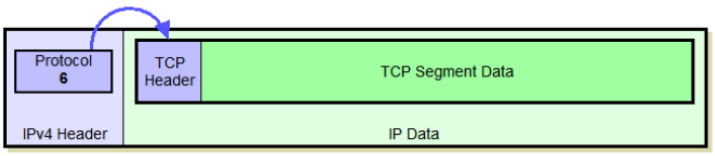
ESP (Encrypted Security Payload) – ESP proporciona los mismos servicios que AH, añadiendo además la confidencialidad.

IPsec puede proporcionar estos servicios en dos modos: modo túnel y modo transporte.

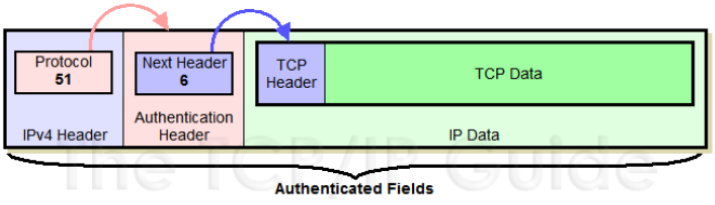
El modo de transporte: En este modo, cada segmento TCP junto con una cabecera (AH o ESP) viaja encapsulados en un datagrama entre el router fuente y el destino.

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.

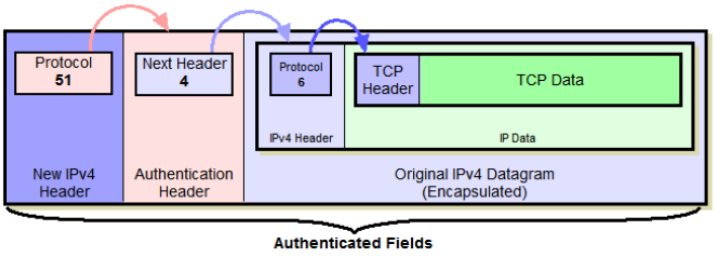
En IPSec modo de transporte la fuente y el destino de la comunicación llevan a cabo los controles de seguridad, por el contrario, en IPSec modo túnel la fuente y el destino no tienen la capacidad ni los recursos para llevar a cabo estos controles de seguridad en los paquetes.



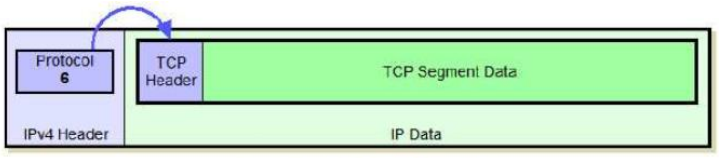
Original IPv4 Datagram Format



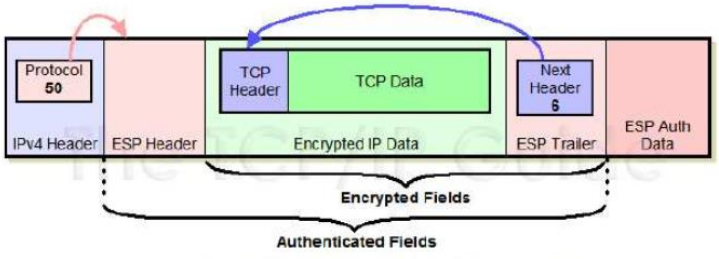
IPv4 AH Datagram Format - IPSec Transport Mode



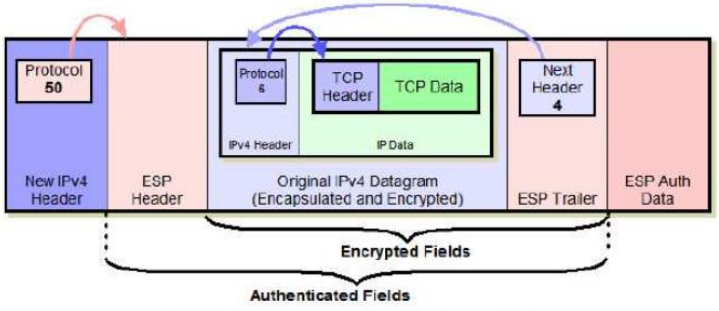
IPv4 AH Datagram Format - IPSec Tunnel Mode



Original IPv4 Datagram Format



IPv4 ESP Datagram Format - IPSec Transport Mode



IPv4 ESP Datagram Format - IPSec Tunnel Mode

Ejercicio 3: VPN con IPsec modo túnel

1. OBJETIVO

Crear una red privada virtual VPN utilizando Packet Tracer simulando una conexión entre dos redes pertenecientes a una empresa RED A y RED B y que tiene conexión a Internet, a través del Router 0.

Se debe permitir a los equipos de la RED A tener acceso a los equipos de la RED B y viceversa, pero se desea que las comunicaciones entre dichas redes se realicen con integridad y confidencialidad.

Para ello se utilizará encriptación y autenticación de datos entre las dos áreas utilizando **IPsec modo túnel**.

2. CREAR LA TOPOLOGÍA DE RED

2.1. Creación de la topología

Vamos a seguir trabajando con el esquema de la **Figura 1.** Por eso, abra el fichero que salvó anteriormente como **P5vpn.pkt** o bien elimine las listas de acceso creadas en los apartados anteriores.

2.2. Verificación de la conectividad

Compruebe la conectividad entre todos los equipos.

3. VPN Y ENCRIPTACIÓN

Una vez configurados todos los equipos adecuadamente y verificado que existe conectividad entre todos ellos, vamos a realizar la encriptación de los paquetes para que las redes A y B realicen comunicaciones con integridad y confidencialidad es decir que el resto (Internet ó Router 0) no conozca el contenido de dichos paquetes:

Pasos:

En Router A:

Configuración de intercambio de claves.

Este proceso usa **ISAKMP** para identificar el algoritmo resumen y el método de autenticación (en este caso usamos clave preacordada). También se identifican los extremos del túnel:

*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***

!--- 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**

*!--- 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**

*!--- 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**

!--- 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**

!--- Crear un 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**

En Router B:

Repetir los pasos haciendo los cambios oportunos, (téngase en cuenta que la configuración es simétrica).

4. MONITORIZACIÓN Y PRUEBAS

4.1 Desde el modo simulación envíe un paquete desde uno de los PC's de la RED A a uno de los PC's de la RED B

Utilice Capture/Forward.
Seleccione uno de los paquetes de la lista de eventos en los que intervenga Router A o Router B como destino y abra así la ventana de información de la PDU y en dicha ventana seleccione la pestaña "Outbound PDU detail".
Localice: "encapsulation security payload" y responda a las siguientes cuestiones:

¿Cómo se encapsulan los datos?

¿Cómo se autentican los datos?

4.2 Verifique que la configuración está funcionando correctamente.

Para comprobar el túnel creado utilice el comando
*Router#***show crypto ipsec sa**

Utilizar el comando debug para comprobar que se establece un canal seguro.
Router# **debug crypto**

4.3 ¿Qué sucede si configuramos de nuevo el Router B pero cambiamos en esta ocasión la clave *vpnuser* por otra? Compruébelo.

GLOSARIO

IPSec: Internet Protocol Security. Es un conjunto de protocolos que se utilizan para proteger las comunicaciones IP. IPSec incluye intercambio de claves y cifrado de túnel. Al crear una VPN IPSec se puede elegir entre una variedad de tecnologías de seguridad.

AH: Authentication Header. Proporciona integridad y autenticación, y evita el ataque por repetición.

ESP: Encrypted Security Payload. Proporciona integridad y autenticación, evita el ataque por repetición y asegura la confidencialidad.

ISAKMP (IKE): Internet Security Association and Key Management Protocol. Proporciona mecanismos para la autenticación en una comunicación segura. Suele utilizar Internet Key Exchange (IKE), pero también se pueden usar otras tecnologías. Se utilizan claves públicas o una clave previamente compartida para autenticar las partes en la comunicación.

MD5: Message Digest 5. (Algoritmo de Resumen del Mensaje 5) es un algoritmo para resumir mensajes de manera criptográficamente segura ampliamente utilizado. La codificación del MD5 de 128 bits se representa típicamente como un número de 32 dígitos hexadecimales.

SHA: Secure Hash Algorithm. Es un conjunto de funciones de resumen criptográfico diseñado por la Agencia de Seguridad Nacional (NSA). Los algoritmos SHA están estructurados de manera diferente y se distinguen como SHA-0, SHA-1 y SHA-2, en función del número de bits del resumen.

DES: Data Encryption Standard. Proporciona cifrado simétrico con una clave de 56-bits. Ya no es considerado un protocolo seguro porque su clave es demasiado corta, lo que lo vuelve vulnerable a ataques de fuerza bruta.

3DES: Triple DES fue diseñado para superar las limitaciones y debilidades de DES usando tres claves diferentes de 56 bits. Los datos se cifran con una clave de 56 bits, a continuación, se descifran con otros 56 bits diferentes y el resultado se vuelve a cifrar con una tercera clave de 56 bit.

AES: Estándar de cifrado avanzado. Fue diseñado para remplazar DES y 3DES. Está disponible en diferentes longitudes de clave y es considerado generalmente como unas seis veces más rápido que 3DES.

HMAC: Hashing Message Authentication Code. Es un tipo de código de autenticación de mensajes (MAC). HMAC se calcula mediante un algoritmo específico que incluye una función de resumen criptográfico en combinación con una clave secreta.