**Ejercicio 6- Creación de una red privada virtual (VPN)**

En la red de la compañía XYZ se tiene que establecer una VPN para cierto tipo de comunicaciones entre las dos sedes principales. Para ello se debe realizar cifrado y autenticación de datos entre las dos áreas utilizando IPsec en modo túnel.

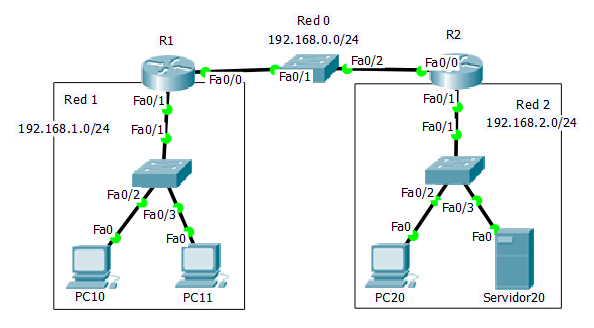


Figura 1. Topología de la red

**Guía de la práctica**

**Tarea 1:** Bajar el fichero de trabajo desde Aula Digital. Utilizando el direccionamiento que se indica completar la configuración de los sistemas de la red.

**Tarea 2:** Comprobar la conectividad entre todos los equipos. ¿Hay conectividad entre todos ellos? En caso que no haya conectividad, resolver el problema.

R: La conectividad no existía inicialmente, faltaba asignar algunas direcciones IP, default gateways y actualizaciones en las tablas de encaminamiento de ambos routers.

**Tarea 3:** Creación de la VPN. Configurar el intercambio de claves en R1. Este proceso usa ISAKMP para identificar el algoritmo de hash y el método de autenticación. También se identifican los extremos del túnel

* Paso 1: Entrar en el modo configuración global del encaminador (*router*) R1
* Paso 2: Creación de una política de *ISAKMP*. Para ello, se define una prioridad de 20. Esta prioridad se utiliza para ordenar la aplicación de las políticas de cifrado cuando existen varias. Aquí se tiene que definir también el método de *hash* y el de autenticación que se va a utilizar. Esto se hace de la forma siguiente a través de la interfaz CLI del IOS:

*R1(config)#crypto isakmp policy 20*

*R1(config-isakmp)#hash md5*

*R1(config-isakmp)#authentication pre-share*

*R1(config-isakmp)#exit*

* Paso 3: Especificación de la clave compartida y de la dirección ip remota (del otro extremo que formará parte del túnel). Especificar la clave “vpnsec” con la que se van a cifrar los datos. Para ello, proceder con el comando siguiente:

*R1(config)#*crypto isakmp key *vpnsec* address 192.168.0.2

* Paso 4: Crear un *transform-set*, por ejemplo, con el nombre “vpnab”. El *transform-set* define las políticas de seguridad IPsec que se aplicarán al tráfico que entra o sale de la interfaz donde se aplica.

R1(config)#crypto ipsec transform-set vpnab esp-des esp-md5-hmac

* Paso 5: Crear una regla ACL para seleccionar el tráfico que se pretende cifrar de la Red 1 a la Red 2 (es decir, el tráfico que se enviará a través de la VPN). Para ello, ejecutar el comando siguiente:

*R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255*

* Paso 6: Creación de un mapa criptográfico. En el ejemplo se le asignará el nombre “mimap”. En este apartado se indica la dirección ip del par del otro extremo de la VPN, la política de seguridad IPsec creada en el paso 4 y la lista de control de acceso (ACL) creada en el paso 5.

R1(config)#crypto map mimap 10 ipsec-isakmp

R1(config-crypto-map)#set peer 192.168.0.2

R1(config-crypto-map)#set transform-set vpnab

R1(config-crypto-map)#match address 100

R1(config-crypto-map)#exit

* Paso 7: Aplicación del mapa criptográfico creado a la interfaz correspondiente, en este caso a la interfaz G0/0. Para ello, proceder de la manera siguiente:

R1(config)#interface G0/0

R1(config-if)#crypto map mimap

R1(config-if)#exit

**Tarea 4:** Repetir los pasos de la tarea 3 para configurar el encaminador R2, realizando los cambios correspondientes (tener en cuenta que la configuración ha de ser simétrica).

**Tarea 5:** Realizar pruebas y visualizarlas con el modo de simulación para comprobar su funcionamiento.

Desde el modo simulación enviar un paquete desde uno de los PC’s de la Red 1 a uno de los PC’s de la Red 2. Utilizar “Capture/Forward”.

Después, seleccionar uno de los paquetes de la lista de eventos en los que intervenga R1 ó R2 como destino y abrir la ventana de información de la PDU; en dicha ventana seleccionar la pestaña “Outbound PDU detail”.

Localizar el siguiente texto: “encapsulation security payload” y responder a las siguientes preguntas:

* ¿Cómo se encapsulan los datos?

R: Se pueden ver dos cabeceras IP, la cabecera Ethernet y el Encapsulating Security Payload.

Texto

Descripción generada automáticamente

* ¿Cómo se autentican los datos?

R: Se autentican a través de ESP con MD5. Se encriptan a través de ESP con DES.

**Tarea 4:** Visualizar la configuración y el funcionamiento desde uno de los encaminadores (*routers*). Para ello proceder según se indica en los pasos siguientes:

* Paso 1: Para comprobar el túnel creado utilizar el comando

R1#show crypto ipsec sa

* **Paso 2:** Utilizar el comando *debug* para comprobar que se establece un canal seguro. Para activarlo utilizar el comando siguiente:

R1# debug crypto ?(para ver las distintas opciones)

**Tarea 5:** Conclusión. Realizar una breve descripción de lo realizado en esta práctica (indicar qué se ha realizado y como, sobretodo centrarse en explicar lo que se ha conseguido desde el punto de vista de la seguridad).

R: Se ha creado una VPN del tipo IPSec en modo túnel entre 2 redes (concretamente entre las interfaces internas de 2 routers separados por un switch).

Desde el punto de vista de seguridad, se ha conseguido confidencialidad e integridad de la información enviada y también autenticación, al aplicar los algoritmos y/o herramientas utilizados por el túnel IPSec.

**(Se acabó la práctica)**

**GLOSARIO**

* **IPSec:** Internet Protocol Security (**IPSec**) es un conjunto de protocolos que se utilizan para proteger las comunicaciones IP. IPSec incluye tanto intercambio de claves y el cifrado del túnel. Al crear una VPN IPSec, puede elegir entre una variedad de tecnologías de seguridad para aplicar el túnel.
* **ISAKMP (IKE):** Internet Security Association and Key Management Protocol (ISAKMP) proporciona un medio para la autenticación de los pares en una comunicación segura. Suele utilizar Internet Key Exchange (IKE), pero otras tecnologías también pueden ser utilizados. Las claves públicas o una clave previamente compartida se utiliza para autenticar las partes en la comunicación.
* **MD5:** Message-algoritmo Digest 5 (MD5) es de uso frecuente para realizar funciones de hash criptográfica. El valor hash es también llamado el resumen del mensaje.
* **SHA:** Secure Hash Algorithm (SHA) es un conjunto de funciones de hash criptográfica 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. SHA-1 es un algoritmo de hash de uso común, con una longitud de clave de 160 bits estándar.
* **ESP:** Carga de seguridad encapsuladora (ESP) es un miembro de la suite de protocolo IPsec que proporciona autenticidad de origen, la integridad, confidencialidad y protección de los paquetes. ESP también soporta el cifrado y la autenticación de sólo-sólo configuraciones, pero utilizar cifrado sin autenticación está totalmente desaconsejado, ya que es inseguro. A diferencia del protocolo IPsec otros, Authentication Header (AH), ESP no protege a la cabecera del paquete IP. Esta diferencia hace ESP preferido para su uso en una configuración de traducción de direcciones de red. ESP opera directamente sobre IP, utilizando el protocolo IP número 50.
* **DES**: El Data Encryption Standard (DES) proporciona encriptación de 56-bits. Ya no es considerado un protocolo seguro porque su clave de corta duración lo hace vulnerable a ataques de fuerza bruta.
* **3DES**: 3DES fue diseñado para superar las limitaciones y debilidades de DES usando tres diferentes claves de 56 bits en una operación de cifrar, descifrar, y volver a cifrar. 3DES claves de 168 bits de longitud. Cuando se utiliza 3DES, los datos es la primera cifra con una clave de 56 bits, a continuación, descifra con un 56 diferentes-bit, el resultado de que luego se vuelve a cifrar con un tercero 56-bit.
* **AES**: El estándar de cifrado avanzado (AES) fue diseñado como un reemplazo para DES y 3DES. Está disponible en diferentes longitudes de clave y es considerado generalmente como unas seis veces más rápido que 3DES.
* **HMAC**: El hashing Message Authentication Code (HMAC) es un tipo de código de autenticación de mensajes (MAC). HMAC se calcula mediante un algoritmo específico que incluye una función de hash criptográfica en combinación con una clave secreta.