| | Carátula para entrega de prácticas | |
|---|---|---|
| Facultad de Ingeniería | | Laboratorios de docencia |

# Laboratorio de Redes y Seguridad

*Profesor:* Ing. Magdalena Reyes Granados

*Asignatura:* Laboratorio de Administración de Redes

*Grupo:* 01

*No de Práctica(s):* Práctica Adicional 06

*Integrante(s):* Gutierrez Silvestre Griselda

Sánchez Bautista Velia

*No. de Equipo de cómputo empleado:*

*Semestre:* *2021-1*

*Fecha de entrega:* *03-11-2020*

*Observaciones:*

CALIFICACIÓN: _____

## PRÁCTICA EXTRA
## Configuración Básica de VPN (Red Privada Virtual)

### *1.- Objetivo de aprendizaje*

- El alumno realizará el análisis y la configuración de una VPN (red privada virtual) empleando el software de simulación de red, Cisco Packet Tracer, Versión Student.

### *2.- Conceptos teóricos*

Una red privada virtual VPN es una red privada construida dentro de una infraestructura de red pública, tal como la red de Internet. Las organizaciones pueden utilizar redes privadas virtuales para conectar de manera segura oficinas y usuarios remotos a través de la red de Internet a costos económicos, proporcionados por terceros en lugar de enlaces WAN dedicados o enlaces de marcación remota a larga distancia, con un costo mucho más elevado.

Las VPN proporcionan el mayor nivel de seguridad posible, mediante seguridad IPsec cifrada o túneles VPN de Secure Socket Layer (SSL) y tecnologías de autenticación.

Estas tecnologías protegen los datos que pasan por la VPN contra accesos no autorizados.

Las VPN extienden la seguridad a los usuarios remotos, proporcionando comunicaciones seguras con derecho de accesos adaptados a usuarios individuales, aumentan la productividad al ampliar el alcance de las redes y reducen los costos de comunicación.

Existen dos tipos de redes privadas virtuales cifradas:

- **VPN IPSec de sitio a sitio:** Esta alternativa a Frame Relay o Redes WAN de línea arrendada, permite a las organizaciones extender los recursos de la red a las sucursales, oficinas, entre otros.
- **VPN de acceso remoto:** Extiende prácticamente todas las aplicaciones de datos, voz o video a escritorios remotos emulando los escritorios de la oficina central. Las redes VPN pueden desplegarse usando redes VPN SSL, IPSec o ambas.

**Funcionamiento de una VPN**

Una VPN se basa en un protocolo denominado “Protocolo de túnel”, es decir, un protocolo que cifra los datos que se transmiten de un lado de la VPN hacia el otro (ver figura 1.1).

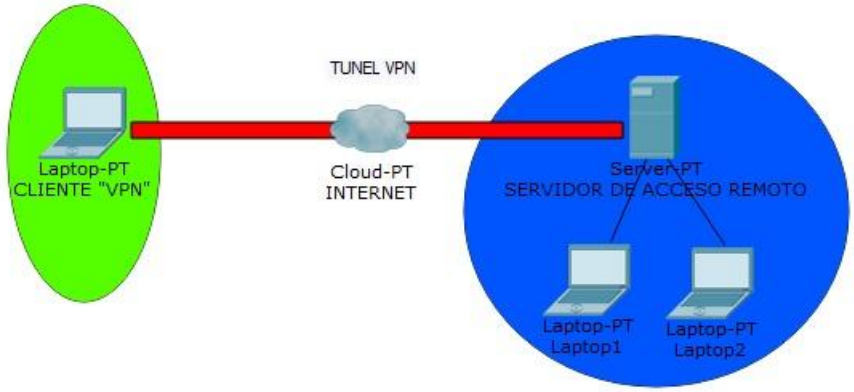


**Figura 1.1 Protocolo de túnel**

La palabra "túnel" se utiliza para representar el hecho de que los datos están cifrados desde el momento que entran a la VPN y hasta que salen de ella.

Los principales protocolos de túnel son:

**PPTP (Protocolo de túnel Punto a Punto):** Protocolo de capa 2 que permite el tráfico seguro de datos desde un cliente remoto a un servidor corporativo privado, estableciéndose así una red privada virtual, basada en TCP/IP. Fue desarrollado por Microsoft, 3com, Ascend, US Robotic y ECI Telematics.

**L2F (Reenvío de capa 2):** Desarrollado por Cisco, para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas. L2F no depende del protocolo IP ya que es capaz de trabajar con otros medios, como Frame Relay o ATM. Actualmente es casi obsoleto.

**L2TP (Protocolo de túnel de capa 2):** Es un protocolo estándar de túnel para Internet, que tiene casi la misma funcionalidad que el protocolo PPTP. L2TP no admite túneles nativos a través de redes X.25 o Frame Relay.

**IPSec (Internet Protocol Security):** Protocolo de capa 3, cuya función es asegurar las comunicaciones sobre el Protocolo IP autenticando y/o cifrando cada paquete IP en un flujo de datos.

## *3.- Equipo y material necesario*

### *3.1 Equipo del Laboratorio*

- Computadora con Windows 7
- Software Cisco Packet Tracer, Version Student.

## *4.- Desarrollo*

### *Modo de trabajar*

La práctica se desarrollará por parejas.

### 4.1 Configuración de una VPN

En esta topología se implementará una conexión VPN entre la SEDE 1 y la SEDE 2.

**4.1.1** Abra el software de simulación Cisco Packet Tracer, Version Student.

**4.1.2** Agregué al área de trabajo los siguientes componentes, así como se muestra en la figura 1.2.

- 3 Routers 1841
- 2 Switch 2950-24
- 2 PC-PT

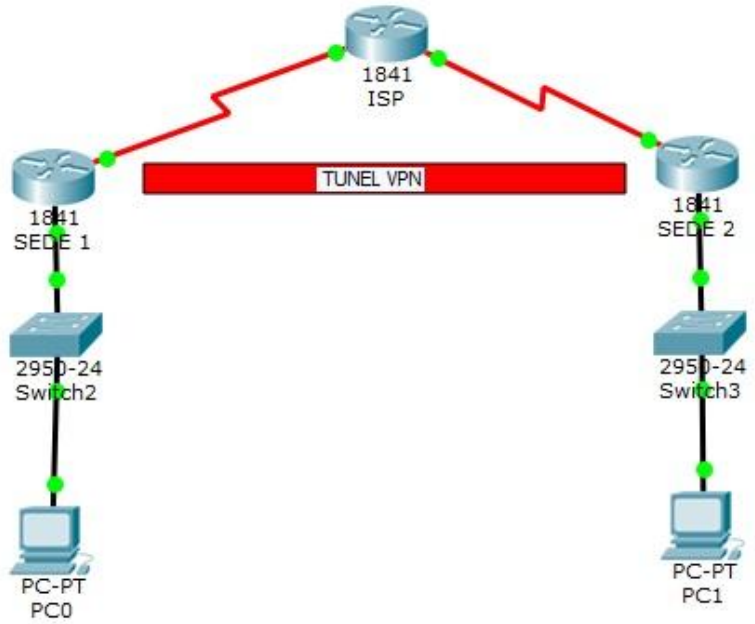


**Figura 1.2 Topología de red.**

**4.1.3** El segmento de red que utilizará será proporcionado por su profesor.

**4.1.4** Realice las configuraciones necesarias para que la topología de red tenga conectividad exitosa, emplee el protocolo de enrutamiento dinámico RIPv2 (ver figura 1.2).

### 4.2 Configuración del Router de la SEDE 1.

Para configurar el router es necesario establecer una política de encriptación, la cual se empleará para proporcionar seguridad de manera compartida, así como las claves de autenticación para los servicios como IPSec.

De igual manera, se requerirán del conocimiento de ciertos comandos para realizar las configuraciones necesarias en cada router, como lo son:

- Protocolo **Isakmp (Asociación de seguridad en Internet y Protocolo de administración de Claves):** Define el mecanismo de implementación de un protocolo de intercambio de claves y la negociación de las políticas de seguridad.
- **Hash:** Función unidireccional que selecciona un mensaje de entrada con una longitud arbitraria y produce un resumen con una longitud fija.
- **SHA (Algoritmo de hash seguro)**: Son algoritmos que consiguen crear a partir de una entrada (texto, contraseña o archivo) una salida alfanumérica de longitud fija que representa un resumen de toda la información que se la ha brindado.
- **AES (Advanced Encription Standard):** Es un esquema de cifrado por bloques adoptado como un estándar de cifrado.
- **Lifetime:** Es el tiempo de vida para la conexión, puede ser entre 60 hasta 86400 segundos.
- **Group**: Puede declarar cual es el tamaño del módulo que se va a utilizar. El grupo 1 tiene una longitud de 768 bits y el grupo 2 tiene una longitud de 1024 bits.
- **Pre-share:** Claves precompartidas que se utilizarán.

Para la configuración del Router de la Sede1 se emplearan los siguientes valores:

- **ID de la política:** 10
- **Algoritmo:** hash

- **Encriptación:** aes de 256 bits
- **Grupo:** group 2
- **Lifetime:** 86400

Para ello, es necesario que ejecute los siguientes comandos:

Sede1>enable
Sede1#configure terminal
Sede1(config)#crypto isakmp policy **ID**
Sede1(config-isakmp)#authentication pre-share
Sede1(config-isakmp)#hash sha
Sede1(config-isakmp)#encryption **aes 256**
Sede1(config-isakmp)#**group 2**
Sede1(config-isakmp)#lifetime **86400**
Sede1(config-isakmp)#exit

- El comando **'transform-set'** define las políticas de seguridad que serán aplicadas al tráfico que entra o sale de la interfaz.
- El estándar **IPSec** especifica el uso de Security Asociations para determinar qué políticas de seguridad se aplicarán al tráfico deseado.
- **Set transform-set:** Asocia las transformaciones con una correspondencia criptográfica.
- **esp-aes**: esp transformado utilizando cifrado AES
- **esp-sha-hmac:** esp tranformado utilizando autenticación HMAC-SHA
- **access-list:** define la lista de control de acceso (ACL) IP, que pueden filtrar el tráfico de la red.
- **crypto-map:** Aplica la correspondencia de criptografía a la interfaz.
- **IPSec (Internet Protocol Security):** Permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autenticación. IPSec posee dos métodos de encriptado, modo transporte y modo túnel. Así mismo, soporta encriptado de 56 bit y 168 bit (triple DES).
- **Match address 101:** significa que se va a emplear la lista de acceso 101 para determinar cuál es el tráfico más destacado.

Valores a utilizar:

**Llave:** CISCO123
**Política de seguridad:** LABREDES

Sede1(config)#crypto isakmp key **CISCO123** address *ip_router_serial_sede2*
Sede1(config)#crypto ipsec transform-set **LABREDES** esp-aes esp-sha-hmac
Sede1(config)#access-list **101** permit ip ***segmento_sede1 wildcard segmento_sede2 wildcard***
Sede1(config)#crypto map **ADMIN 10** ipsec-isakmp
Sede1(config-crypto-map)#set peer *ip_serial_sede2*
Sede1(config-crypto-map)#**match address 101**
Sede1(config-crypto-map)#set transform-set **LABREDES**
Sede1(config-crypto-map)#interface serial ***id_serial***
Sede1(config-if)#crypto map **ADMIN**
RouterSede1(config-if)#exit

**4.2.1** Realice las configuraciones para el Router de la Sede2, apoyándose de los comandos del router de la Sede1. El identificador de la política de acceso debe ser igual en ambos routers, así como su correspondiente ACL.

### *4.3 Cuestionario*

1.- ¿Cuáles fueron los principales problemas que obtuvo al realizar las configuraciones correspondientes en cada router? ¿Cómo los resolvió?

Unicamente tuvimos problemas en el router ya que ese modelo no contaba con una interfaz serial para conectarlos entre sí. Se resolvió agregando una interfaz.

Ejecute y analice cada uno de los siguientes comandos en el router Sede1 y Sede2:

**show crypto isakmp sa**

Nos indica que la autenticación se realizó de forma exitosa, y las asociaciones del protocolo isakmp creadas entre los pares

**show crypto isakmp policy**

Nos muestra el algoritmo ha ash usado, el método de autenticación

**show crypto ipsec sa**

muestra detalles como el crypto map que se está utilizando y dónde esta aplicado , el tráfico que pasa a través del túnel

**show crypto map**

Nos muestra las SA IPsec generadas entre peers, se muestra de igual forma el tráfico pasado por los routers pero está cifrado

### *5.- Conclusiones*

Revise los objetivos de la práctica y las actividades realizadas y emita sus conclusiones.

Gutierrez Silvestre Griselda

El protocolo VPN nos permite establecer conexiones seguras a través de un medio inseguro. Ya que nos permite garantizar confidencialidad, integridad y autenticación. En este caso se usó un cifrado AES de 256 bits, un intercambio de llaves por el grupo Diffie-Hellman, un hashing sha y el metodo de autenticación psk.

Sánchez Bautista Velia

Los objetivos de la práctica se cumplieron, partiendo de una topología y sus configuraciones, usamos IPsec que nos permitió establecer una comunicación segura garantizando la integridad, la confidencialidad y la autenticación.

Bibliografía:
https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html