2023

TRABAJO DE LABORATORIO Nº 4

Configuración Avanzada de Routers y Redes Privadas Virtuales

ACTIVIDAD DE FORMACION PRACTICA

1. Formación experimental (laboratorio).

OBJETIVOS

1. Incrementar las habilidades para configurar dispositivos routers con funciones de enrutamiento entre VLANs e implementando una red WAN que conecte dos redes LAN, con diferentes protocolos de enrutamiento dinámico, rutas estáticas y rutas por defecto.
2. Comprender la arquitectura de las redes privadas virtuales (VPN), analizando los diferentes casos básicos de acceso remoto seguro, desde un host externo hacia una LAN propia.
3. Familiarizar al alumno con el empleo de los documentos técnicos del fabricante para realizar la configuración de un acceso VPN con el protocolo IP Sec, así como la implementación de ACLs extendidas para "tunelizar" o "filtrar" paquetes IP.
4. Aplicar los métodos apropiados para la solución de problemas de configuración.

CONOCIMIENTOS PREVIOS

1. Arquitectura básica de VPN.
2. Configuración de routers, switches y VLANs (prácticas anteriores).
3. Operación y uso del software de simulación.
4. Conocimiento de las estructuras de datos y funcionamiento de IPSec.
5. Lectura comprensiva de los siguientes temas teórico-prácticos: Redes IP, Redes Privadas Virtuales en Internet, Extranet e Intranet, Protocolo IPSec, Protocolo GRE, Túneles de Capa 2 con PPTP y L2TP, Firewall basado en filtros de paquetes IP con ACL ampliadas o extendidas, Seguridad con Clave Simétrica, Protocolo IKE (Internet Key Exchange), Firma digital con SHA y HMAC, Cifrado con AES, Algoritmo Diffie-Hellman.
6. Diseño detallado de filtros de paquetes con ***access control list (ACL) extendidas*** y verificación mediante prueba de escritorio.
7. **EJERCICIOS RESUELTOS DE LAS GUÍAS DE EJERCICIOS DE ESCRITORIO (GEE):**

9.3.1. a 9.3.3	Configuración
9.7.1	Configuración
9.9.2.	Configuración

MATERIAL NECESARIO

1. Para las **ACTIVIDADES PREVIAS**:
   a. Archivos **1cfrip.pdf**, **1cfigrp.pdf** y **1cfeigrp.pdf**, de Cisco System, a fin de integrarlo con el conocimiento de enrutamiento desarrollado en los archivos ***Enrutamiento.pdf*** y ***13769-5.pdf (TL 3)***.
   b. Archivos ***75923_confaccesslists.pdf (TL 3)***, ***ACL.pdf*** *y* ***sec-data-acl-xe-3s-book.pdf***.
   c. Guía de Configuración ***Network Design Considerations – Cap 2***, de Cisco System.
   d. Archivo en **Samples Files:\Security\Ipsec2.pkt**, ejemplo de funcionamiento de una VPN basada en túnel *IPSec*, disponible en simulador ***Packet Tracer, versión empleada en laboratorio***.
2. Para el desarrollo del ***Caso de Estudio***:
   a. Una PC de escritorio con el simulador ***Packet Tracer versión indicada para los Laboratorios***, instalado.
   b. Archivos TL4-Configuración avanzada de Routers-2022.pkt, Conf VPN ISP.txt, Conf VPN R2.txt.

ACTIVIDADES PREVIAS

1. Realice un repaso de los conocimientos prácticos desarrollados en los TL 1 a 3, con especial atención a VLANs, ampliando su conocimiento al enrutamiento entre VLANs mediante routers, desarrollado en el archivo ***14976-50_interVLAN routing on router.pdf***.
2. Haga una lectura comprensiva de los archivos ***1cfrip.pdf***, ***1cfigrp.pdf*** *y* ***1cfeigrp.pdf***, de Cisco System, a fin de integrarlo con el conocimiento de enrutamiento desarrollado en los archivos ***Enrutamiento.pdf*** y ***13769-5.pdf (TL 3)***.
3. Profundice el estudio del diseño e implementación de filtros de paquetes IP con ACL extendidas, en base a los archivos ***75923_confaccesslists.pdf (TL 3)***, ***ACL.pdf*** *y* ***sec-data-acl-xe-3s-book.pdf***.
4. Analice las consideraciones de diseño para VPNs, en base al documento ***Network Design Considerations – Cap 2***, archivo ***6342ch2.pdf***, comprendiendo los diferentes escenarios de uso (**Overview of Business Scenarios)** y, de manera detallada, los aspectos técnicos descriptos sobre el modo Túnel IPSec (**Hybrid Network Environments, Integrated versus Overlay Design, Network Traffic Considerations)**.
5. Realice un estudio profundo de las modalidades de configuración VPN, en particular lo descripto en el documento **Site-to-Site and Extranet VPN Business Scenarios – Cap 3**, archivo ***6342cmbo.pdf***.
6. Amplíe el conocimiento de VPN mediante la lectura reflexiva del documento **Remote Access VPN Business Scenario – Cap 4**, archivo ***6342rmt.pdf***.

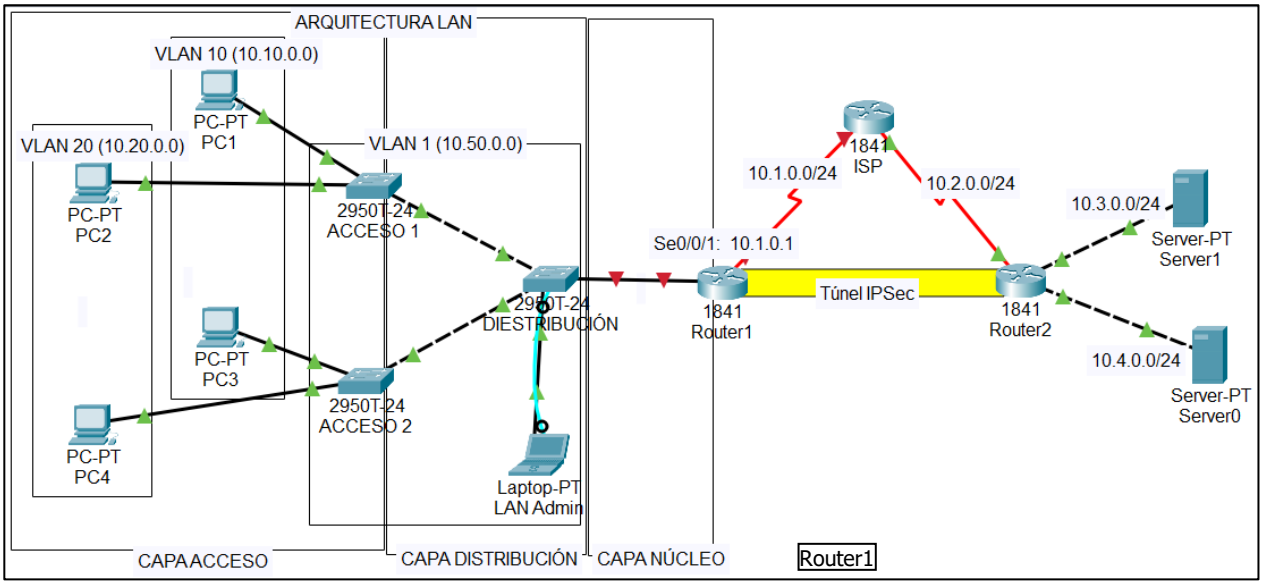
DESCRIPCION

Este trabajo será desarrollado por los alumnos de manera individual, utilizando el simulador **Cisco Packet Tracer**, aplicando la situación inicial del escenario previamente configurado en el archivo TL4-Configuración avanzada de Routers-2022.pkt.

1. Caso de Estudio

Se requiere el establecimiento de un túnel IPSec entre 2 sucursales de una empresa (Router1 con Router2), con la topología que se indica en la siguiente figura.

Caso de Estudio - TOPOLOGÍA



2. Requerimientos para el alumno (Objetivos Técnicos)

a. **Realizar las operaciones de configuración de los dispositivos (router, switch, etc) de manera correcta.**
b. **Utilizar correctamente las funciones de configuración del software.**
c. **Demostrar la comprensión del funcionamiento de los protocolos considerados en la actividad de laboratorio, mediante la verificación experimental del modelo y proceso descripto en la teoría y en las RFCs respectivas.**

3. Configuración de la red

Paso 1: **COMPLETAR Y VALIDAR LA TOPOLOGÍA PARA EL LABORATORIO**

1) En el simulador conecte los medios y dispositivos, según el Caso de Estudio.
2) En configuración de PCs y dispositivos utilice el diseño IP dado, considerando las VLANs indicadas.

Paso 2: **CONFIGURACIÓN BÁSICA DE LOS ROUTERS**

1) Realizar la configuración de las interfaces del router R1 y el enrutamiento dinámico con EIGRP para el SISTEMA AUTÓNOMO 1, más una ruta por defecto a la IP del ISP respectiva y probar la conectividad entre los mismos a través del ISP.
2) Las dos sucursales de la empresa cuentan con conexiones de banda ancha e IP fija, según lo indicado en el gráfico.
3) Las redes LAN y VLAN utilizan direccionamiento privado de diferentes subredes. El ISP asegura la conectividad entre las IP públicas.
4) Ya se encuentran realizadas las configuraciones de los routers ISP y R2, así como los servidores S0 y S1.

Paso 3: **CONFIGURAR LA VPN EN EL ROUTER 1**

Analice los comandos y utilícelos como referencia para su aplicación en el modo de configuración global o específico que corresponda. **Los datos (parámetros) en cada caso, no han sido incluidos en esta guía**, con la finalidad de que el alumno los defina en base a lo estudiado en los documentos técnicos y a la configuración dada del Router2.

1) **Configuración de 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 una cabecera de autenticación más cifrado (Encapsulating Security Payload o ESP).

```
conf t
crypto isakmp policy 10
encr AES
authentication pre-share
group 5 (Diffie-Hellman grupo 5 – clave de 1536 bits)
lifetime 900 (tiempo de vida en segundos)
exit
```

Notas técnicas:

- crypto isakmp policy **10**: *este comando crea la política ISAKMP número 10. Puede crear varias políticas, por ejemplo 7, 8, 9 con una configuración diferente. Los routers que participan en la negociación de la Fase 1 buscan la coincidencia de políticas ISAKMP con la lista de políticas una por una. Si alguna política coincide, la negociación de IPSec pasa a la Fase 2.*
- encr **AES**: *se utilizará el algoritmo AES para la fase 1.*
- authentication pre-share: *el método de autenticación es una clave pre-compartida.*
- group **5**: *el grupo Diffie-Hellman que se utilizará es el 5 (grupo de 1536 bits).*
  Los grupos Diffie-Hellman (DH) determinan la fuerza de la clave usada en el proceso de intercambio de claves. Los miembros de grupos más altos (DF 14, 15, 19 y 20)son más seguros, pero se necesita más tiempo para computar la clave. Ambos puntos en un intercambio de VPN deben usar el mismo grupo DH, que es negociado durante la Fase 1 del proceso de negociación de IPSec. Es ahí donde los dos puntos forman un canal seguro y autenticado que pueden usar para comunicarse.
- lifetime **900**: *tiempo de vida en segundos.*

Definición de una clave simétrica con el otro extremo del túnel:

```
crypto isakmp key cisco address 10.2.0.2
```

(La contraseña de la fase 1 es "cisco" y la dirección IP remota es 10.2.0.2)

2) **Configuración de IPSec modo túnel**

```
crypto ipsec transform-set 50 ah-sha-hmac esp-3des
```

(Para listar las otras opciones de autenticación y encriptación utilice el comando *crypto ipsec transform-set **50** ?*)

- **crypto ipsec transform-set 50** – Crea un conjunto o mapa de transformación llamado 50 (en este caso)

3) **Configurar la lista de acceso para determinar tráfico de origen y destino del túnel. La VLAN 10 es la única que deberá encaminarse por el túnel IPSec; las**

otras deberán ser filtradas mediante ACLs extendidas, en origen.

- **Para el túnel:**
  access-list **101** permit ip **10.10.0.0 0.0.255.255 10.4.0.0 0.0.0.255**
- **Para las restantes VLANs, se hará por similitud, utilizando las guías respectivas.**

4) **Configurar el mapa que determina la IP del extremo remoto del túnel y el tráfico de interés que será encapsulado.**

crypto map **mymap 10** ipsec-isakmp
set peer **10.2.0.2**
set security-association lifetime seconds **1800**
set transform-set **50**
match address **101**

Notas técnicas:

- **crypto map mymap 10 ipsec-isakmp:** *crea un nuevo mapa criptográfico con el número de secuencia 10. Puede crear más números de secuencia con el mismo nombre de mapa criptográfico si tiene varios sitios.*
- **set peer 10.2.0.2:** *Es la dirección IP pública del router del otro extemo del túnel.*
- **set security-association lifetime seconds 1800:** *Establece en 1800 segundos el tiempo de establecimiento de la asociación de seguridad.*
- **set transform-set NOMBRE** - *Esto vincula el conjunto de transformación en esta configuración de mapa criptográfico.*
- **match address 101:** *determina el tráfico de la ACL 101 que será el admitido en el túnel.*

5) **Activar el túnel**

int **se0/0/1**
crypto map **mymap**

Paso 4: **CONFIGURAR LAS VLANS EN EL ROUTER 1 Y SWITCHES DE LA ARQUITECTURA LAN**

Paso 5: **PROBAR LA RED, TANTO MEDIANTE EL TÚNEL COMO LOS RESTANTES SEGMENTOS PERMITIDOS Y FILTRADOS.**

TIEMPO ASIGNADO: 120 minutos

CRITERIO DE EVALUACION

Se aprobará el TLab, si se alcanzan los siguientes resultados:

1. Ejecución correcta de las actividades experimentales y logro de los objetivos técnicos.
2. Respuestas satisfactorias a evaluaciones orales individuales sobre situaciones de configuración o análisis.
3. Demostración al docente del funcionamiento correcto de la configuración requerida mediante un PING, TRACERT o NAVEGACIÓN WEB.