2022 - AUTOEVALUACION DE ACTIVIDADES DE FORMACION PRÁCTICA

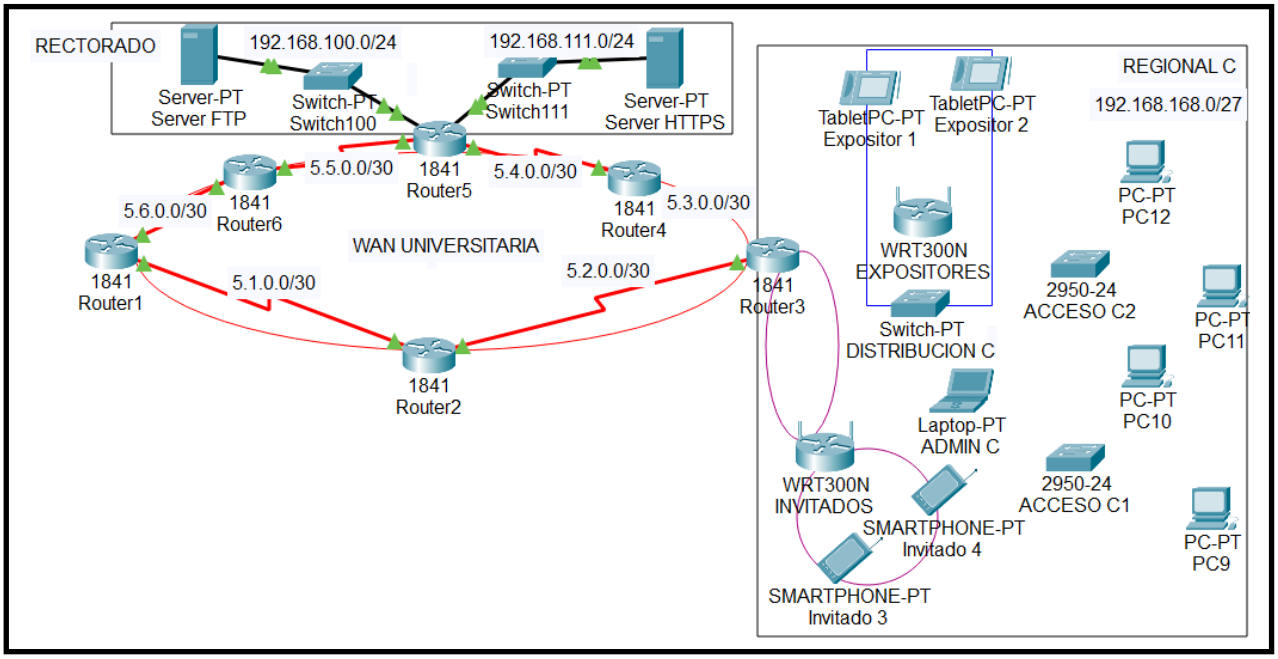
TL 1234 - ESCENARIO C 2

OBJETIVO DE LA AUTOEVALUACIÓN (DURACIÓN 120 MINUTOS)

Que el alumno compruebe de manera autónoma su conocimiento práctico en la implementación de accesos seguros a servicios autorizados de una red corporativa que interconecte dos LAN mediante enlaces WAN (en ambiente de laboratorio con simulador), demostrando habilidades en:

- Configuración de computadoras y dispositivos móviles para acceso a la LAN o VLAN.
- Configuración de control de acceso a dispositivos de red.
- Configuración de Access Point como bridge entre el segmento WLAN y el segmento cableado.
- Configuración de Access Point como router entre el segmento WLAN y el segmento cableado.
- Configuración de enrutamiento dinámico en todos los routers del escenario (RIP v2, IGRP, EIGRP).
- Configuración de enrutamiento por defecto y estático en routers.
- Configuración de Túnel IPSec entre 2 redes LAN remotas.
- Configuración de enrutamiento de VLANs hacia la WAN (dentro del túnel IPSec o fuera de él).
- Configuración de filtros de paquetes con ACL extendidas en un router.
- Identificación y resolución de problemas de networking.
- Resolución de problemas de networking mediante el estudio de los documentos técnicos ofrecidos por el fabricante.

CASO DE AUTOEVALUACIÓN



MÍNIMO RESULTADO REQUERIDO

1.1. Completar la configuración con los requerimientos exitosos en no más de 120 minutos
1.2. Demostrar la COMUNICACIÓN CORRECTA EN LAS VLANs (ping exitoso o no, según corresponda).
1.3. Demostrar el FUNCIONAMIENTO CORRECTO DEL ENRUTAMIENTO (dinámico y estático) en su ROUTER (tabla de enrutamiento).
1.4. Demostrar el FUNCIONAMIENTO CORRECTO DEL TUNEL IPSEC (trazabilidad del paquete).

INFORMACIÓN DEL CASO

1.1. ADMINISTRACION Y SEGURIDAD DE DISPOSITIVOS DE RED

- **NOMBRE:** acorde al gráfico, para cada switch y router de la REGIONAL
- **ADMINISTRACIÓN DE CONFIGURACIÓN (enable):** contraseña **redes**
- **MEDIDAS DE SEGURIDAD DEL ROUTER3**
  - **ACCESO REMOTO CON SSH (vty):** cada dispositivo debe admitir **1 solo acceso remoto con SSH** y tener bloqueados el resto de las líneas y cualquier otro protocolo de acceso remoto.
    - USUARIO: **regional**
    - CONTRASEÑA: **utn**
  - **CONTRO DEL ACCESO REMOTO AL PUERTO VTY:** se debe mejorar la seguridad de la línea administrativa habilitada mediante la restricción del acceso a VTY, permitiendo acceder remotamente **solo con SSH** desde la **Laptop ADMIN C**.

1.2. DATOS LAN LOCAL

- **REGIONAL:** C
- **ARQUITECTURA DE SERVICIOS Y ACTIVOS:**
  - CAPA ACCESO: switch ACCESO C1 (PC9 y PC10), switch ACCESO C2 (PC11 y PC12), Laptop ADMIN B (acceso indistinto).
  - CAPA DISTRIBUCIÓN: 1 Switch
  - CAPA NÚCLEO: 1 router en WAN
- **RED LAN IP:** 192.168.168.0/27
  - **RED VLAN 77 (ALUMNOS) IP:**
    - SUBRED 192.168.168.32/27
    - PCs: 9 y 11
  - **RED VLAN 88 (DOCENTES) IP:**
    - SUBRED 192.168.168.64/27
    - PCs: 10 y 12
  - **RED VLAN 99 (ADMIN) IP:**
    - SUBRED 192.168.168.128/27
    - Laptop: ADMIN C
  - **RED WLAN (EXPOSITORES):**
    - Direccionamiento IP necesario (puede ser con VLSM) para **conmutar** 2 dispositivos móviles (Expositor 1 y Expositor 2) por **bridging** a la **VLAN 88 (DOCENTES)** mediante **DISTRIBUCION C**.
    - SSID: Exp0s1tor35, canal 8.
    - Contraseña Autenticación WPA2-PSK: **M4sr3str1ctivA.-**
    - Contraseña Confidencialidad AES.
    - TabletPC: Expositor 1 y Expositor 2.
- **RED ACCESS POINT (INVITADOS) IP:** 192.168.170.0/24
  - Direccionamiento IP segmento WLAN (192.168.180.0/24) para **conmutar** hasta 100 celulares (Invitado 3 e Invitado 4) por **routing** hacia el servidor **HTTPS del RECTORADO**, fuera del túnel IPSec mediante el **ROUTER 3**.
  - SSID: 1nv1t4d0s, canal 13.
  - Contraseña Autenticación WPA2-PSK: **much0+fu3rt3**
  - Contraseña Confidencialidad AES.
  - TabletPC: Invitado 3 e Invitado 4, deben tener acceso al servidor HTTPS del RECTORADO.

1.3. DATOS WAN UNIVERSITARIA

- **PROTOCOLO FÍSICO:** SERIE, SINCRÓNICO, CLOCKING 2.000.000, FULL DUPLEX.
- **PROTOCOLO DE ENLACE HACIA LAS REGIONALES:** PPP (Todos los enlaces de la WAN Universitaria)
- **PROTOCOLO DE RED:**

- **Direccionamiento:** IP, CON SUBREDES **5.1.0.0/30 A 5.6.0.0/30**, de acuerdo con los enlaces y la topología del gráfico.
- **Enrutamiento: RIP versión 2**. La ruta por defecto se deberá dirigir hacia el **Router 4**.
- **Seguridad**:
  - Túnel IPSec entre los routers 3 y 5 (clave isakmp: **redes**) para permitir que el acceso de los docentes (VLAN 88) a los servicios del SERVIDOR HTTPS se encaminen por el túnel IPSec. El extremo del túnel del lado RECTORADO debe terminar sobre la interfaz WAN.
  - Los protocolos criptográficos para el túnel IPSec se adoptarán en base a la configuración del Router 5, al cual podrá acceder por TELNET.
  - Fuera del túnel, SÓLO DEBE PERMITIRSE el acceso por FTP de la Laptop ADMIN de la Regional al server FTP (192.168.100.100, Username: **usuarioseguro** / Password: **contraseñasegura**) del RECTORADO. Todo el resto del tráfico de la Regional debe ser denegado en origen, **excepto los INVITADOS del segmento WLAN que deben poder acceder al servidor HTTPS del RECTORADO**.

- **NETWORKING:**
  - **Las configuraciones de los dispositivos del escenario, NO SON CONFIABLES.**
  - **Los problemas de convergencia en la WAN por necesidades de redistribución de protocolos de enrutamiento, en caso de ser necesario, deberán ser resuelto por los alumnos, investigando el tema en el sitio del proveedor (**https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html**) u otras referencias académicas.**
    - **Todos los problemas detectados deberán ser solucionados por el administrador, en modo local o remoto.**

1.4. **OTROS DATOS**: Serán definidos por el usuario o el docente ATP de cada curso.