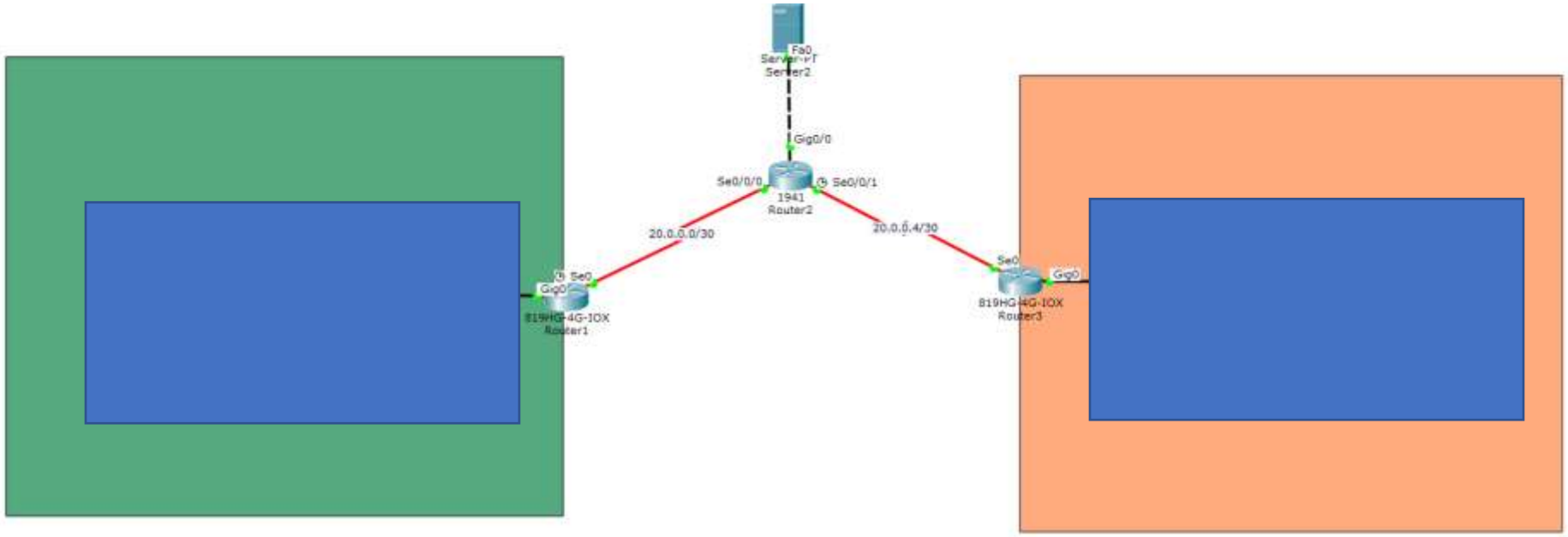
Universidad Don Bosco, El Salvador. Facultad de Estudios Tecnológicos Escuela de Computación			
Ciclo / Año:	02-2017.	Grupo Teórico:	TODOS.
Fecha:		Grupo Laboratorio:	TODOS.

Caso de Estudio #2.

1. Investigue en proceso de configuracion de una VPN de sitio a sitio protegida por medio de IPSec, para realizar el proceso de este caso de estudio tome como base la siguiente información
    a. La topología deberá emular la interconexión de dos sitios remotos a través de Internet utilizando VPN IPSec



    b. La VPN deberá ser establecida para proteger el tráfico de red entre las redes de los extremos, Todo el tráfico que sea ajeno a lo anteriormente establecido no deberá estar protegido por el filtrado.
    c. El servidor mostrado en la topología anterior simula el internet, por lo que se debe de hacer el proceso de configuración necesario para que el entorno funcione como se espera (Ambas redes pueden alcanzar internet, pero este tráfico no estará protegido).

Haciendo uso de CISCO PACKET TRACER, diseñe e implemente la topología de red que cumpla con los siguientes requerimientos de conectividad y seguridad:

- **d.** En el Sitio 1, los siguientes segmentos de red existen
  - **i.** Red de usuarios (550 direcciones IP)
  - **ii.** Red de Servidores Críticos (50 direcciones IP)
  - **iii.** Red de Servidores accesibles desde Internet (5 direcciones IP)
  - **iv.** Red Pública (16 direcciones IP)
- **e.** En el Sitio 2, los siguientes segmentos de red existen
  - **i.** Red de usuarios (150 direcciones IP)
  - **ii.** Red Pública (4 direcciones IP)
- **f.** Utilizando la técnica de VLSM, deberá subnetear la dirección de red 172.16.60.0/20 para asignar los segmentos de red que correspondan al sitio 1. Y la dirección de red 10.10.10.0/24 para el sitio 2
- **g.** Las redes de usuarios deberán tener acceso a la red pública (Internet) haciendo uso de la primera IP pública para el Sitio 1 y la segunda IP pública para el Sitio 2, (Deberá realizar el proceso de NAT o PAT según sea su criterio).
- **h.** Todos los servidores críticos tendrán acceso a Internet, través de la tercera dirección IP pública del segmento correspondiente
- **i.** Cada uno de los 5 Servidores accesibles desde Internet deberá utilizar su propia IP pública para acceder a Internet
- **j.** Los servicios que serán accesibles desde Internet son los siguientes:
  - **i.** Servidor 1: HTTP y HTTPS
  - **ii.** Servidor 2: SSH, SMTP, POP3
  - **iii.** Servidor 3: SFTP
  - **iv.** Servidor 4: Microsoft RDP
  - **v.** Servidor 5: DNS
- **k.** Cada segmento de red deberá estar separado lógicamente entre sí, a través del uso de Interfaces o sub-interfaces del router o firewall
- **l.** Las siguientes reglas de control de acceso deberán cumplirse:
  - **i.** Toda la red de usuarios (en ambos sitios) tendrá acceso únicamente a los siguientes servicios en la red de servidores críticos: HTTP, DNS, HTTPS, Active Directory, SFTP, UDP/4547, TCP/33456, TCP/7777, TCP/445

ii. Únicamente el personal de tecnología de la organización, quienes utilizan las últimas 15 direcciones IP del segmento de red asignado en cada sitio, podrá acceder a los siguientes servicios en la red de servidores críticos: SSH, Microsoft RDP, TCP/8081, SNMP, ICMP

iii. Únicamente el Servidor 1 (de la red de servidores accesibles desde Internet) podrá tener acceso a través del puerto TCP/1433 hacia el servidor de base de datos de la red de servidores críticos

iv. Solo el personal de tecnología de ambos sitios podrá acceder a través de los protocolos: SSH, Microsoft RDP, TCP/8081, SNMP, ICMP; a los servidores de la red de servidores accesibles desde Internet

v. Solo el servidor de correo electrónico de la red de servidores críticos podrá comunicarse con el Servidor 2 de la red de servidores accesibles desde Internet y viceversa

vi. El Servidor 4 de la red de servidores accesibles desde Internet deberá tener acceso a través del puerto TCP/8085 hacia el servidor de base de datos de la red de servidores críticos

vii. Todos los Servidores accesibles desde Internet podrán acceder a través del servicio de Active Directory a los dos servidores definidos como Controladores de Dominio en el segmento de red de los servidores críticos

viii. El acceso a Internet de todos los usuarios, en ambos sitios, será controlado en el Sitio 1 y los únicos protocolos permitidos son los siguientes: HTTP y HTTPS. El Sitio 2 no debe permitir el acceso a Internet a los usuarios que allí se encuentran

ix. Los servidores de la red crítica no deberán tener acceso a la red de usuarios ni a la red de servidores accesibles desde Internet

m. Utiliza como pool de direcciones públicas a 168.243.3.0/29.