UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA
ESCUELA DE ELECTRÓNICA

Asignatura:	**Diseño de sistemas de seguridad en redes de datos**	Código:	**DSS101**
Grupos:	**01L, 02L, 03L, 04L, 05L y 06L**	Ciclo / año:	**02 - 2020**

CASO DE ESTUDIO #3
"Sistema de seguridad perimetral con firewalls"

Condiciones de realización:

Fecha de Entrega:	**Semana 15 (03 - 07/11/2020)**
Porcentaje:	15%
Forma de Entrega:	Demostración de funcionamiento de la solución durante la sesión de laboratorio. Documento en PDF a ser subido en el aula digital, el documento debe contener evidencias de configuraciones y funcionamiento del sistema.
Grupos:	4 personas

Descripción de la actividad:

Haciendo uso de GNS3 y máquinas virtuales (si no cuenta con el hardware necesario, puede hacer uso de Packet Tracer), los estudiantes deben implementar mecanismos de seguridad perimetral utilizando Firewalls, el diseño de seguridad consiste en la configuración de direccionamiento IP, NAT, VPN, ACLs. La topología de red que se detalla en el diagrama de red de la figura 1. Los requerimientos de seguridad solicitados se detallan a continuación:

a. Crear un plan de direccionamiento IP para la asignación de las direcciones a cada interfaz de los firewalls, interfaz del router, servidores y PC2.
b. Aplicar enrutamiento en los dispositivos de red para pueda existir comunicación en toda la red.
c. Configurar NAT en los Firewalls para asegurar las zonas de interés.
d. Se debe crear una VPN entre los firewalls FW1 y FW2 donde se encriptará toda comunicación entre PC2 y los servidores de la red interna. La comunicación de PC2 hacia el servidor FTP 2 no debe ser encriptada.
e. El servidor FTP 2 deberá ser accesible desde la PC2 (subir y descargar archivos) y deberá responder a las pruebas de PING.
f. Únicamente el WWW Server de la red de servidores de red interna deberá ser capaz de comunicarse con el servidor FTP 2 (descargar archivos).
g. El servidor FTP 2 no deberá comunicarse (acceso a servicios) ni con el EMAIL Server ni con el FTP Server, excepto a través de tráfico ICMP para diagnosticar problemas de conectividad.
h. PC2 deberá poder conectarse hacia EMAIL Server para el envío de correo y descarga de correo haciendo uso de los protocolos SMTP y POP3.

i. El FTP server deberá ser capaz de conectarse a las consolas de administración de FW1, FW2 y RT1; para realizar tareas de configuración haciendo uso del protocolo SSH y diagnóstico de la conectividad a través del protocolo ICMP.

j. Documentar las configuraciones realizadas en los firewalls FW1, FW2 y en el Router RT1.

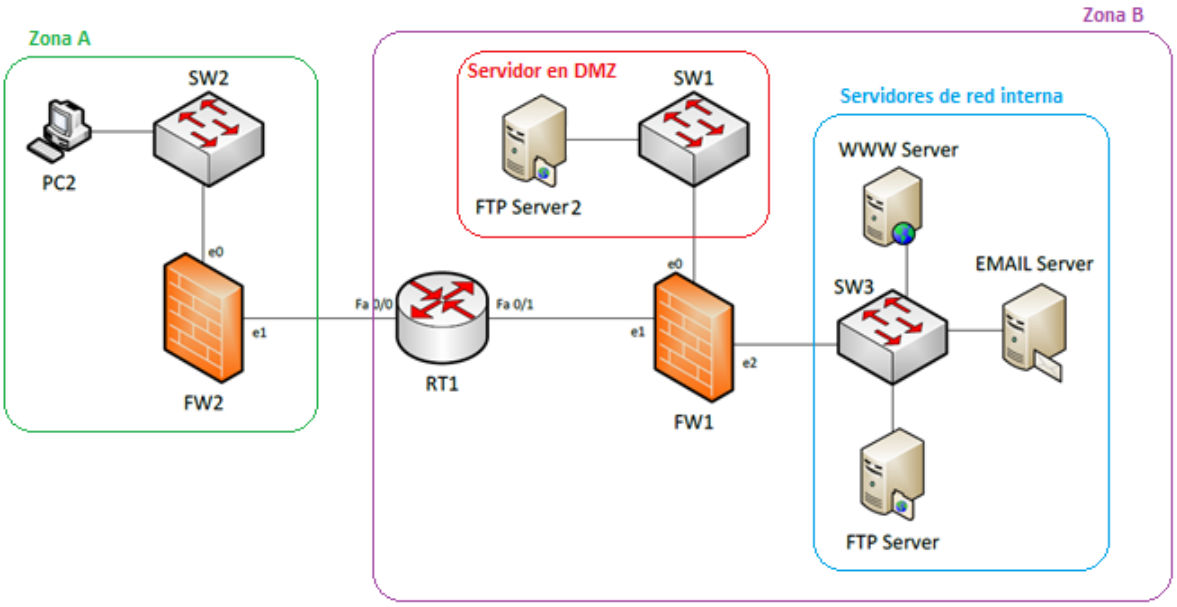

Figura 1. Topología de red.

Lista de estimación:

Actividad a evaluar	Criterio a evaluar	Porcentaje (%)	Puntaje (0-10)
Configuración inicial de red	Crea un plan de direccionamiento IP y aplica las direcciones a cada interfaz de los firewalls, del router, servidores y PC2.	5	
	Configura enrutamiento en los dispositivos de red para pueda existir comunicación en toda la red.	5	
Mecanismos de seguridad perimetral	Configura NAT en los Firewalls para asegurar las zonas de interés.	10	
	Crear una VPN entre los firewalls FW1 y FW2 para asegurar la comunicación entre PC2 y los servidores de la red interna. La comunicación de PC2 hacia el servidor FTP 2 no debe ser encriptada.	15	
	Configura una ACL para que el servidor FTP 2 sea accesible desde la PC2 (subir y descargar archivos). Además, el servidor FTP 2 deberá de responder a las pruebas de PING desde PC2.	10	

	Configura una ACL para que únicamente el WWW Server de la red de servidores de red interna sea capaz de comunicarse con el servidor FTP 2 (descargar archivos).	10	
	Configura una ACL para que el servidor FTP 2 no pueda comunicarse (acceso a servicios) con el EMAIL Server ni con el FTP Server, excepto a través de tráfico ICMP para diagnosticar problemas de conectividad.	10	
	Configura una ACL para que PC2 pueda conectarse hacia EMAIL Server para el envío de correo y descarga de correo haciendo uso de los protocolos SMTP y POP3.	10	
	Configura una ACL para que el FTP server sea capaz de conectarse a las consolas de administración de FW1, FW2 y RT1; para realizar tareas de configuración haciendo uso del protocolo SSH, además debe permitir el diagnóstico de la conectividad a través del protocolo ICMP.	10	
Documentación de las configuraciones realizadas	Presenta un archivo de texto con las configuraciones realizadas en FW1	5	
	Presenta un archivo de texto con las configuraciones realizadas en FW2	5	
	Presenta un archivo de texto con las configuraciones realizadas en RT1	5	
		Promedio:	