Universidad AUTÓNOMA de Occidente	**UNIVERSIDAD AUTONOMA DE OCCIDENTE**			
	FACULTAD DE INGENIERIA ***NÚCLEO MIDIA***	**NOMBRE DE LA ASIGNATURA**	*Servicios Telemáticos*	
	CODIGO:	**NOMBRE:**		***Valoración***
SEGUNDO PARCIAL			FECHA ASIGNACIÓN: septiembre 18 de 2023 FECHA SUSTENTACIÓN: septiembre 26 de 2023	

PRIMERA PARTE	**Evaluación Teórica (2.0 Puntos)**	PUNTAJE	

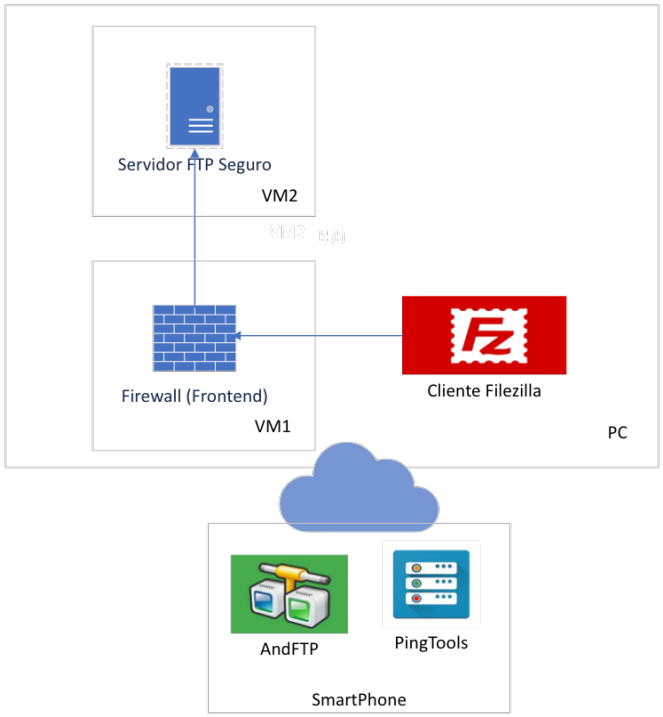
Temas: correo electrónico, servicios seguros, firewall. Parcial disponible en UAO virtual el martes 26 de septiembre a las 6:30 pm. (en punto).

SEGUNDA PARTE	**Evaluación Practica (3.0 Puntos)**	PUNTAJE	

Entrega: martes 26 de septiembre, en los horarios disponibles en el sitio del curso

PARTE 1: FTP SEGURO (1.5 Puntos)

Implemente la topología mostrada en la figura:



Requerimientos:

[0.5 Puntos] Servicio 1: Firewall

1. Todas las solicitudes de acceso a los servicios implementados deben ser canalizadas a través del firewall designado como punto de entrada y seguridad en la red. En ningún caso se permitirá el acceso directo a los servicios configurados sin pasar por el firewall.

2. En el caso específico del servicio FTP Seguro, se exige que los clientes utilicen el firewall como intermediario obligatorio para redirigir sus solicitudes al servidor FTP Seguro correspondiente.

[0.5 Puntos] Funcionamiento de FTP Seguro

1. La implementación debe incluir una demostración desde un dispositivo Smartphone que demuestre que el servidor FTP está operando de manera segura. Esto implica la utilización de un cliente de FTP seguro en el Smartphone, que debe poder establecer una conexión y realizar transferencias de archivos de forma segura y encriptada.

2. Se requiere una prueba adicional, similar a la anterior, pero realizada desde un equipo anfitrión, utilizando un cliente FTP seguro como Filezilla u otro equivalente. Debe demostrarse que el servidor FTP Seguro puede ser accedido de manera segura desde un dispositivo anfitrión, garantizando así la integridad y confidencialidad de las transferencias de archivos.

[0.5 Puntos] Clientes: PC Anfitrión, Smartphone

1. Es esencial llevar a cabo las pruebas de funcionamiento de los servicios implementados desde dos tipos de dispositivos distintos: un PC anfitrión y un Smartphone.

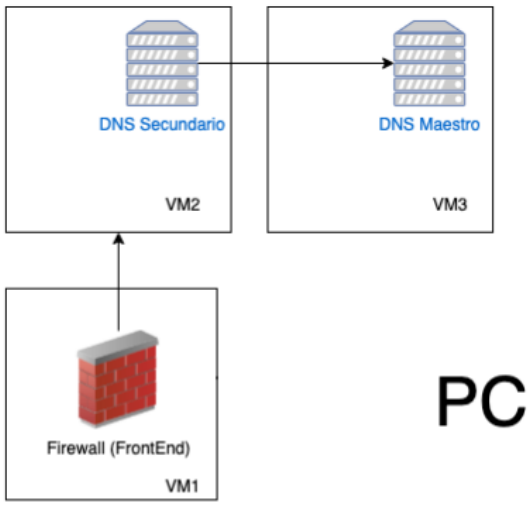
2. Ambos dispositivos deben ser capaces de acceder al FTP Seguro, utilizando los clientes adecuados.

3. Estas pruebas se deben realizar con el objetivo de verificar y documentar que los servicios operan según lo esperado, sin vulnerabilidades evidentes y proporcionando los niveles de seguridad requeridos para proteger la integridad y la confidencialidad de los datos transferidos.

Estos requerimientos son esenciales para garantizar la correcta implementación y funcionamiento de un servidor FTP Seguro, y para demostrar que dicho servidor cumple con los estándares de seguridad necesarios al canalizar todas las solicitudes a través del firewall y proporcionar acceso seguro desde múltiples dispositivos.

PARTE 2: DNS MAESTRO/ESCLAVO PROTEGIDO POR FIREWALL (1.5 Puntos)

Implemente la topología mostrada en la figura:



Requerimientos:

[0.5 Puntos] Servicio 1: Firewall

Todas las solicitudes de acceso a los servicios configurados deben ser dirigidas al firewall designado como punto de entrada y seguridad en la red. En ningún caso se permitirá el acceso directo a los servicios sin pasar por el firewall. En el caso específico del servicio DNS, se exige que los clientes utilicen el firewall como intermediario obligatorio para redirigir sus solicitudes al servidor DNS correspondiente, garantizando así la centralización y control del tráfico DNS.

[1.0 Puntos] Servicio 2: DNS Maestro/esclavo

1. Se requiere la implementación de un sistema de Servidores DNS que comprenda un servidor DNS maestro y un servidor DNS esclavo. El servidor maestro deberá ser capaz de realizar transferencias de zona al servidor esclavo de manera efectiva.
2. Para la configuración de las máquinas virtuales en el laboratorio, se empleará el nombre corto **"nombre_empresa"** como el dominio de referencia.
3. Cada máquina virtual deberá configurar el servidor DNS predeterminado para utilizar el servidor DNS configurado en la máquina virtual 2 (VM2).
4. Es fundamental realizar pruebas para verificar que, dada la resolución de nombres de dominio de cada equipo dentro del laboratorio, el servidor DNS pueda resolver de manera adecuada las direcciones IP asociadas, independientemente de la máquina desde la cual se realice la prueba.

Seleccione un nombre corto para su empresa (**nombre_empresa)** y configure las maquinas virtuales con los nombres de dominio y los servicios descritos en la siguiente tabla:

Maquina	Servicio	Nombre de Dominio	Descripción
VM 1	Firewall	firewall.nombre_empresa.com	Máquina virtual con el servicio firewalld instalado
VM 2	DNS secundario	servidor2.nombre_empresa.com	Máquina virtual con el servicio named instalado
VM 3	DNS maestro	servidor3.nombre_empresa.com	Máquina virtual con el servicio named instalado

NOTA:
Si su máquina tiene recursos limitados, puede plantear una topología con 2 máquinas virtuales en lugar de una. Tenga en cuenta que el DNS maestro y el esclavo deben funcionar en máquinas separadas.

EVALUACIÓN

Valor	Descripción	Puntaje Obtenido
2.0	Evaluación teórica	
1.5	FTP seguro	
1.5	DNS maestro/esclavo	
	TOTAL	