Universidad AUTÓNOMA de Occidente	**UNIVERSIDAD AUTONOMA DE OCCIDENTE**			
	FACULTAD DE INGENIERIA *DEPARTAMENTO DE AUTOMATICA Y ELECTRONICA*		**NOMBRE DE LA ASIGNATURA**	*Servicios Telemáticos*
	CODIGO:	**NOMBRE:**		***Valoración***
SEGUNDO PARCIAL			FECHA ASIGNACIÓN: septiembre 19 de 2022 FECHA SUSTENTACIÓN: septiembre 27 de 2022	

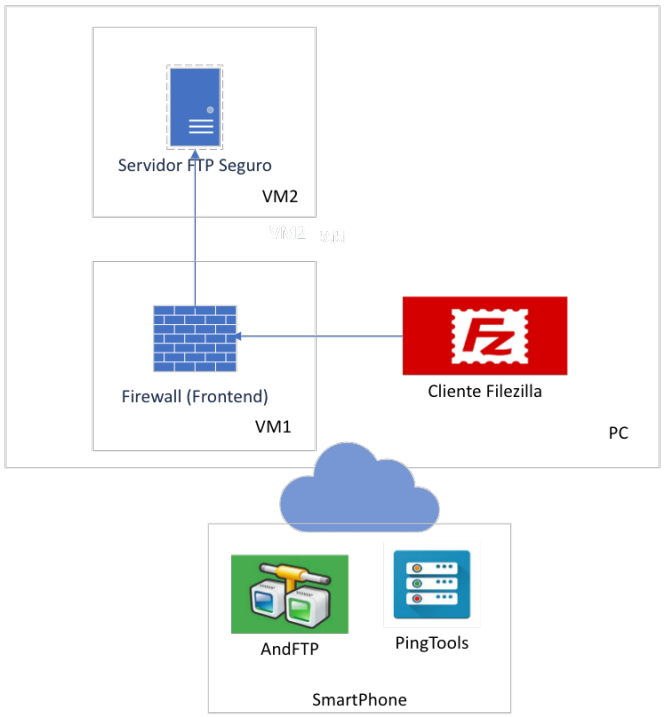
PRIMERA PARTE	**Evaluación Teórica (2.0 Puntos)**	PUNTAJE	

Temas: correo electrónico, servicios seguros, firewall. Parcial disponible en UAO virtual el martes 27 de septiembre a las 6:30 pm. (en punto).

SEGUNDA PARTE	**Evaluación Practica (1.5 Puntos): FTP Seguro protegido por firewall**	PUNTAJE	

Entrega: martes 27 de septiembre, en los horarios disponibles en el sitio del curso.

Implemente la topología mostrada en la figura:



Requerimientos:

[0.5 Puntos] Servicio 1: Firewall

Todas las solicitudes deberán ser realizadas al firewall y en ningún caso directamente a los servicios configurados. Si se requiere usar el servicio FTP Seguro, el cliente deberá hacerlo a través del firewall y redirigirlo al servidor FTP Seguro.

[0.5 Puntos] Funcionamiento de FTP Seguro

1. Desde el Smartphone, demuestre que el servidor de FTP funciona de manera segura
2. Realice la misma prueba del punto anterior pero ahora desde el anfitrión (usando Filezilla u otro cliente).

[0.5 Puntos] Clientes: PC anfitrión, Smartphone

Se debe realizar la prueba de los servicios desde un Smartphone y desde el PC anfitrión. Compruebe el funcionamiento de los servicios implementados.

TERCERA PARTE	**Evaluación Practica (1.5 Puntos): DNS over TLS**	PUNTAJE	

[1.0 Puntos] Implementación de DNS over TLS

Configure un cliente DNS de manera segura usando TLS. Se sugiere guía anexa (sin garantía ni soporte)

[0.5 Puntos] Automatización y Aprovisionamiento

Utilice los servicios de aprovisionamiento que provee Vagrant usando Shell para el servicio de DNS over TLS quede aprovisionados de manera automática.

CUARTA PARTE	(OPCIONAL) RichRules **[Hasta 0.5 Puntos adicionales]**	PUNTAJE	

Valido por hasta 0.5 Puntos adicionales.

Investigue el concepto de Rich Rules de firewalld e implemente un ejemplo donde se usen.

EVALUACIÓN

Valor	Descripción	Puntaje Obtenido
2.0	Evaluación teórica	
1.5	FTP seguro protegido por Firewall	
1.5	DNS over TLS	
0.5	Opcional	
	TOTAL	

ANEXOS

Habilitar DNS sobre TLS en Linux usando Systemd

Objetivo
Configurar un cliente DNS de manera segura usando TLS

Configuración de la Máquina

Configure una maquina Vagrant con el siguiente Vagrantfile

```
# -*- mode: ruby -*-
# vi: set ft=ruby :

Vagrant.configure("2") do |config|


  if Vagrant.has_plugin? "vagrant-vbguest"
    config.vbguest.no_install  = true
    config.vbguest.auto_update = false
    config.vbguest.no_remote   = true
  end


  config.vm.define :dnstest do |dnstest|
    dnstest.vm.box = "bento/ubuntu-20.04"
    dnstest.vm.network :private_network, ip: "192.168.20.2"
    dnstest.vm.hostname = "dnstest"
  end

end
```

Configuración del Servicio

Paso 1: Instalar NetworkManager

```
sudo apt-get update
sudo apt-get install network-manager
```

Paso 2: Ver el estado del servicio

```
$ resolvectl status
```

Debe obtener la configuracion por defecto, asi:

```
$resolvectl status
Global
       LLMNR setting: no
MulticastDNS setting: no
  DNSOverTLS setting: no
      DNSSEC setting: no
    DNSSEC supported: no
```

Paso 3: Configurar system-resolved asi:

```
$ sudo vim /etc/systemd/resolved.conf
```

```
[Resolve]
DNS=1.1.1.1 1.0.0.1
FallbackDNS=8.8.8.8 8.8.4.4
```

```
Domains=~.
#LLMNR=no
#MulticastDNS=no
DNSSEC=yes
DNSOverTLS=yes
#Cache=yes
#DNSStubListener=yes
#ReadEtcHosts=yes
```

Paso 4: Reinicie los servicios

```
$ sudo systemctl restart systemd-resolved
$ sudo systemctl restart NetworkManager
```

Paso 5: Verificar la configuracion

```
$ resolvectl status
```

Debe obtener algo como:

```
$ resolvectl status
Global
       LLMNR setting: no
MulticastDNS setting: no
  DNSOverTLS setting: yes
      DNSSEC setting: yes
    DNSSEC supported: yes
  Current DNS Server: 1.1.1.1
         DNS Servers: 1.1.1.1
                      1.0.0.1
Fallback DNS Servers: 8.8.8.8
                      8.8.4.4
          DNS Domain: ~.
```

Paso 6: Verificar en Wireshark

Abrir Wireshark y capture en la interfaz de la red local de su anfitrión, filtrando por tcp.port == 853

Luego ejecute lo siguiente y verifique las transaciones de DNS sobre TLS

```
$ sudo resolvectl flush-caches
$ resolvectl query google.com
```

Analice y explique los mensajes capturados por Wireshark.

Referencias

Enable DNS Over TLS in Linux using Systemd. https://medium.com/@jawadalkassim/enable-dns-over-tls-in-linux-using-systemd-b03e44448c1c

DNS over TLS - Que es y como activarlo en Linux. https://www.youtube.com/watch?v=Nmfw5E7ltAM&t=5s