

Documentació de la infraestructura i arquitectura del Fog

Grup B2 - Terminal2

Sprint 2

Index

1	Disseny de la infraestructura final	2
1.1	Serveis del nostre fog	2
1.2	Recursos utilitzats	3
2	Implementació del servei <i>SSH</i>	4
2.1	Arxius modificats	4
2.2	Securització	4
3	Implementació del servei <i>DHCP</i>	5
3.1	Arxius modificats	5
3.2	Securització	5
4	Implementació del <i>Bridge amb connectivitat WiFi</i>	6
4.1	Arxius modificats	6

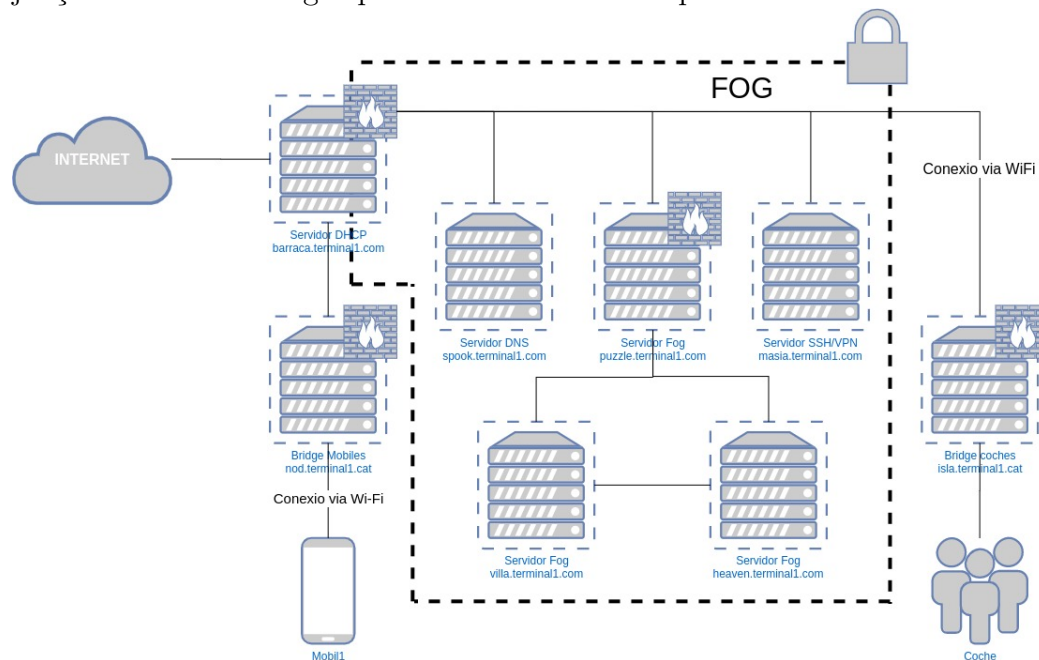
1 Disseny de la infraestructura final

1.1 Serveis del nostre fog

Els serveis que oferim al nostre fog seran aquestos:

- DHCP
- DNS
- SSH
- Conectivitat WiFi per als dispositius:
 - Mòbils
 - Coches

Aquestos serveis ja consensuats ens permetran oferir connectivitat a internet als usuaris de la nostra xarxa ademes de oferir la possibilitat de connexió mitjançant un sistema segur per als administradors que treballin desde casa.



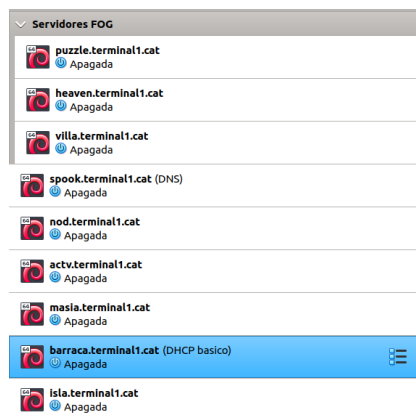
Com poden observar, lis hem donat noms distintius als nostres servidors per així poder ferlos més fàcilment recordables. En el nostre cas hem utilitzat noms referents a discoteques de la *Ruta del Bakalao* de Valencia.

- DHCP es *barraca.terminal1.cat*
- DNS es *spook.terminal1.cat*
- SSH es *masia.terminal1.cat*
- Bridge per als mobils es *nod.terminal1.cat*
- Bridge per als cotxes es *isla.terminal1.cat*
- Fog son:
 - *heaven.terminal1.cat*
 - *puzzle.terminal1.cat*
 - *villa.terminal1.cat*

1.2 Recursos utilitzats

Per permetrens la construccio fisica i d'aquest disseny de arquitectura hem decidit hostejar tots aquestos serveis a una maquina local dintre de la xarxa local de casa.

Aixo ho podem realitzar gracies a la eina *VirtualBox* desenvolupada per *Oracle*.



Com poden observar ja tenim creades totes les maquines virtuals dintre de nostra maquina local. Aquestes maquines correran el sistema operatiu **Debian 10.3** amb *4,00 GB* de disc dur i *512 MB* de ram. Ademes hem creat una xarxa interna amb el nom *terminal1.cat* sense servei de *DHCP*, donat que l'implementarem nosaltres.

Per ultim tambe comentar l'utilització de l'adaptador *WiFi*: *TP-Link TL-WN821N* que ens permetra conectarlo al nostre sistema operatiu i crear una zona *WiFi* per la conexio dels aplicatius mòbils i els coches que es connectin inalambricament.

2 Implementacio del servei *SSH*

Per la instal·lació i creació del nostre servei de *SSH* hem utilitzat el paquet de *Debian*, ***OpenSSH***.

Aquest paquet ens permetrà establir una connexió mitjançant els protocols *SSH*, *SFTP* i *SCP*. A més de ser una de les bases d'un altre servei que implementarem en sprints futurs com pot ser *OpenVPN*.

2.1 Arxius modificats

Els arxius de configuració es troben dintre de la carpeta */etc/sshd/*, on hem editat l'arxiu de configuració d'aquest servei (*sshd.conf*), amb els següents paràmetres (apart dels per defecte):

- `PermitRootLogin prohibited-password`
- `Subsystem sftp internal-sftp`

Aquests dos paràmetres ens permetran l'utilització de l'eina *internal-sftp* per poder compartir arxius internament i per permetre la connexió al superusuari mitjançant *keys* per permetre l'identificació.

2.2 Segurització

Per últim sol tenim que editar el nostre firewall (en el nostre cas el paquet *iptables*) per permetre sol la connexió del protocol *SSH* via el port **22**.

Això ho podem aconseguir canviant la política per defecte de la taula *INPUT* per ***DROP*** e incluent l'acceptació dels paquets entrants per el port **22** i els paquets amb la connexió ja establerta.

3 Implementació del servei *DHCP*

Per l'instal·lació i creació del nostre servei de *DHCP* i permetre així que aquesta màquina virtual realitzi la funció de **router** hem realitzat l'instal·lació del paquet de *Debian*, *isc-dhcp-server*.

Aquest paquet ens permet assignar adreces *IP* mitjançant el protocol *DHCP* per així poder establir una connexió entre aquest router i les màquines internes de la nostra xarxa.

Com es pot veure a la presentació, aquest servidor contaria amb 2 interfícies de red, una per permetre la connexió amb l'exterior (amb connectivitat a internet) i una altra per permetre la connexió amb l'interior de la xarxa, per així poder donar suport a les màquines creades.

3.1 Arxius modificats

Els arxius de configuració es troben dintre la carpeta */etc/dhcp/*, on hem modificat l'arxiu *dhcpcd.conf* i hem indicat quins es el nostre domini de la red, els servidors *DNS* per defecte i l'adreça del router. Ademés també hem establert les subnets (per fer aquesta demostració, es una subnet única) indicant el rang d'adreces disponibles, la màscara de xarxa i el router per defecte.

A més, també hem indicat que treballarem amb un servei de *DNS* dinàmic, per tant, tenim aquest servei cada cop que renti una adreça *IP* a un servidor amb entrada al *DNS* te que actualitzar-la.

3.2 Securització

En aquest cas, la securització a tingut que ser més robusta, donat que es la porta de entrada a la nostra xarxa i es per on poden venir un major nombre de atacs.

Així que hem decidit denegar qualsevol entrada de paquets via l'interfície connectada a Internet amb l'excepció dels paquets amb connexió ja establerta, i els paquets que es vulguin connectar al servidor *SSH* (els quals hem redirigit).

4 Implementació del *Bridge amb connectivitat WiFi*

Donat que treballarem amb dispositius mòbils (en el dos sentits de la paraula) necessitarem implementar una màquina que realitzi la funció de pont entre l'interfície *ethernet* i una xarxa inalàmbrica.

Per això ens hem vist en la necessitat de crear una *Acces Point* amb un adaptador de red a una màquina virtual. En el nostre cas, com ja he explicat anteriorment, utilitzarem el *TP-Link TL-WN821N*.

4.1 Arxius modificats

En primera instància, tenim que instal·lar els drivers del nostre adaptador, connectar-lo a la màquina virtual i comprovar que efectivament, el nostre sistema operatiu ens el detecta.

Després, tindrem que instal·lar-nos el paquet ***hostapd*** juntament amb ***bridge-utils***. El primer paquet ens permetrà la creació d'un punt d'accés *WiFi* i el segon ens permetrà establir un *bridge* entre la interfície *ethernet* i la interfície inalàmbrica.

Els arxius modificats per part del paquet *hostapd* es troben dintre de la carpeta: */etc/hostapd*. En contraposició, el paquet per crear el *bridge* sol hem tingut que modificar l'arxiu */etc/network/interfaces/* i habilitar el *Proxy ARP* i el reenviament de paquets *IPv4*.

L'arxiu principal de la zona *WiFi* es el *hostapd.conf*, on hem indicat el tipus de seguretat que tindrem dintre de la nostra zona (*WPA2-PSK*), l'*ESSID* (terminal1) i la contrasenya (*12345678*) a més d'altres coses (obviament, abans de sortir de l'àmbit de proves, canviarem la contrasenya de la *wifi* i la posarem sense per permetre la connectivitat a tothom).

4.2 Securitització

En aquest cas la securització ha estat mínima, únicament hem modificat el reenviament de paquets de *DNS* per que es realitzi de manera interna. Hem volgut deixar-ho amb el menor nombre de regles possibles perquè creiem que al ser una interfície d'utilització pública (per els usuaris de l'aplicació i tothom que es trobi dintre de la terminal) els usuaris podem connectar-se als serveis externs que desitgin (sempre que el firewall del *DHCP* s'ho permeteixi).