Pràctica 3

Sessió 1 i 2 - Encaminament i tallafocs

Alumnes:
Mariona Farré Tapias,
Marc Pérez Guerrero

CARPETA VMS:
https://drive.google.com/drive/folders/1tsIsl3Bdj11sQhLxI6L4WpaD6Xe4feOx?usp=sharing
---

ÍNDEX:

Enunciat:

1 – Descripció de les xarxes
Xarxa troncal:
Descripció: xarxa "real" des d'on es pot accedir a Internet.
IP: x.y.z.u/m (assignada per DHCP)
Interfícies: eth-troncal
Xarxa DMZ
Descripció: zona desmilitaritzada on ubicar servidors DNS&SSH accessibles des d'Internet i les altres xarxes i el servidor Nagios.
IP: 10.1.10.0/28
Interfícies: eth-dmz
Xarxa clients:
Descripció: xarxa dels usuaris genèrics, amb els equips client de treball.
· IP: 10.1.20.0/24
· Interfícies: eth-clients

2 – Descripció dels equips (entre parèntesis el seu nom DNS)
· Router d'accés (routeracces)
· Funció: connectar amb la xarxa troncal i aïllar del trànsit no desitjat
· Interfícies
· eth-troncal -> IP: x.y.z.u - MAC: 08:00:27:00:00:01 -Internet
· eth-dmz -> IP: 10.1.10.1 - MAC: 08:00:27:01:10:01 - entremig
· Serveis: encaminament, tallafocs, NAT i SSH.

· Router intern (routerintern)
· Funció: interconnectar xarxes internes i protegir/restringir les xarxa de clients
· Interfícies
· eth-dmz -> IP: 10.1.10.2 - MAC: 08:00:27:01:10:02 - entremig
· clients -> IP: 10.1.20.1 - MAC: 08:00:27:01:20:01 -clients
· Serveis: servidor DHCP, encaminament, tallafocs, NAT i SSH.

· Servidors DNS i SSH (2 equips)
· Funció: servidor de noms de domini
· Interfícies
· eth-dmz (dns1) -> IP: 10.1.10.3 - MAC: 08:00:27:01:10:03
· eth-dmz (dns2) -> IP: 10.1.10.4 - MAC: 08:00:27:01:10:04
· Serveis: Oferirà resolució de noms del domini seax.edu i de la seva zona inversa. També del domini "public.edu" (veure enunciat sessió 3). Seran accessibles via SSH.

. Servidor Nagios (nagiosserver)
· Funció: monitorització de tots els elements de la xarxa i d'alguns serveis externs. Visible a través d'una interfície Web.
· Interfícies
· eth-servers -> IP: 10.1.10.5 - MAC: 08:00:27:01:10:05
· Serveis: Nagios i SSH.

· Monitor de xarxa.
Màquina de l'administrador de xarxa. El seu nom, i adreça IP, canvia en funció de la xarxa on es troba (monitoradmin, monitordmz, monitorclients).
· Funció: màquina a disposició de l'administrador de la xarxa per a fer les tasques que cregui convenients.
· Interfícies
· eth0 -> IP: x.y.z.11 - MAC: 08:00:27:01:00:11
· Serveis: SSH.

. Altres equips fora de l'escenari
. El domini "public.seax.edu" tindrà les següent relació de noms i adreces IP que es troben al cloud
+ www -> IP: 147.83.2.135
+ www -> IP: 2001:40b0:7500:1::21

3 – Directrius de seguretat per a la configuració dels tallafocs
- Tots els equips que formen part de l'escenari
+ Han de poder fer-se pings entre ells
+ En general, només poden fer servir els DNS de la DMZ
+ Han de poder ser monitoritzats des del servidor Nagios

- Xarxa clients
+ Ha de poder accedir a serveis externs sense restriccions sempre que no impliquin connexions noves ni paquets que no siguin resposta a una petició prèvia.

- Xarxa DMZ
+ Només els DNS1 i DNS2 són accessibles des de l'exterior
+ Només DNS1, DNS2 i el servidor Nagios poden fer consultes a servidors DNS externs

- Monitors
+ Només ells tenen accés al servei de SSH de la resta d'equips
+ S'ha de poder accedir al seu servei de SSH
++++ Des de qualsevol xarxa interna o externa pel monitor de la DMZ
++++ Des de la xarxa DMZ en el cas del monitor de la xarxa clients

+ Només els monitors tenen accés a la web del servidor Nagios

- Tallafocs
+ Cal maximitar la seva seguretat
+ Cal portar un control del nombre de paquets acceptats
+ Tots els accessos per SSH han de ser registrats
++++ Cal diferenciar si són intents des d'equips permesos o no

- Servidors de DNS
+ S'ha de maximitar la seva seguretat

+ S'hi podrà accedir des de qualsevol xarxa interna o externa

- Servidor Nagios
+ S'ha de maximitar la seva seguretat
+ S'hi podrà accedir des de la mateixa xarxa DMZ o la de clients

4- Directrius de seguretat específiques pels servidors

- Prohibir l'accés al servei durant 5 minuts a les màquines des d'aquelles IPs que han intentat accedir a un servei autenticant-se malament fins a 3 vegades seguides.

5- Accés als serveis de la DMZ des de l'exterior

- Pel servei de DNS es configurarà com un balancejador de càrrega, de manera que en un accés s'accedirà a un dels dos servidors i en el següent a l'altre.

- Pel servei de SSH del monitor s'utilitzarà el port 1234

6 - Tasques a realitzar
· Crear els routers amb la configuració descrita.
· Crear el monitor de xarxa amb la configuració descrita.
· Per cadascun dels routers i tenint en compte la seva ubicació (accés o intern):
    (1) activar la funcionalitat d'encaminament i configurar les rutes necessàries,
    (2) configurar les funcionalitats de tallafocs i traducció d'adreces de xarxa si s'escau,
    (3) Fer les proves pertinents per comprovar que la configuració és operativa.
· Assegurar-se que els routers en arrencar tenen activada la funcionalitat d'encaminament, les rutes i la configuració del tallafocs.
· Apliqueu les directrius de seguretat específiques pels servidors pel monitor i (opcional) els dos routers.

7- Verificar el seu bon funcionament

(Nota: aquesta verificació s'ampliarà en la resta de sessions).
. Comproveu que les interfícies de xarxa dels equips tenen el nom que toca.
. Comproveu que els interfícies de xarxa dels equips tenen la configuració IP que toca.
. Comproveu que les taules d'encaminament dels routers estan complertes.
. Comproveu la connectivitat entre totes les xarxes que formen l'escenari.
. Comproveu que l'accés als serveis i la connectivitat estan limitats d'acord amb les directives de seguretat indicades.
. Comproveu que els tallafocs registren les activitats que se li han encomanat.
. Comproveu que des de l'exterior es pot accedir als serveis de DNS i SSH
. Comproveu que des de l'interior el servei de SSH només és accessible pels monitors.
. Comproveu que des de la xarxa clients hi ha accés a Internet
. Comproveu que el balanceig de càrrega entre els servidors DNS de la DMZ es produeix.
. Comproveu que la redirecció del port 1234 cap el servidor SSH del monitor de la DMZ es produeix.

. Comproveu que es prohibeix l'accés a un servei des d'una adreça IP que s'ha autenticat 3 vegades seguides malament.

8- Lliurar els resultats
Mitjançant Atenea (2 fitxers):
- Redactar l'informe de la pràctica p3_s1_s2_cognom1_nom.txt.
- Realitzar les proves necessàries per justificar els resultats i encapsular els fitxers necessaris en el fitxer p3_s1_s2_cognom1_nom.zip.

Mitjançant Google Drive (màquines virtuals)
- Compartir amb xxx una carpeta a Google Drive (UPC) amb les VMs dels 2 routers i el monitor.
Important:
- L'informe de la pràctica ha de contenir l'enllaç a la carpeta amb les VMs.
- Les VMs han de contenir una còpia de l'informe al directori /root.

9- A títol orientatiu el resultat de la pràctica cal que doni resposta a les següents qüestions:

- Quina configuració (nombre, tipus d'adaptador i xarxa interna a la que estan connectats si és el cas) tenen les màquines virtuals de l'escenari?
- Com es configuren els noms de les interfícies a les màquines de l'escenari?
- Com es configura un router per a que actuï com a tal? Com s'afegeixen rutes estàtiques a un equip?
- Quina és la taula d'encaminament de cadascun dels routers del escenari? Hi ha com a mínim una ruta per a cada xarxa?
- Quin és el router per defecte de cada xarxa? Quin és el router per defecte de cada router?
- Per a cadascuna de les màquines de l'escenari, quin tipus de configuració (estàtica, dinàmica, dinàmica amb reserva) dels paràmetres bàsics per tenir connectivitat IP cal fer? Raona el motiu.
- Quines comunicacions es permeten entre cadascuna de les xarxes (Internet, DMZ, clients)?
- De manera particular, quines accions s'han fet per a maximitzar la seguretat?
- Com es configuren els tallafocs per filtrar paquets d'acord amb les comunicacions que es permeten?
- Com es configura el tallafocs per a registri una determinada activitat?
- Com es configura el tallafocs per a que comptabilitzi el trànsit que passa per una determinada regla?
- Com es configura el tallafocs per a balancejar càrrega entre dos servidors?
- Com es configura el tallafocs per a redirigir un port?
- Com es configura el tallafocs per a connectar una xarxa a Internet compartint l'adreça IP del router de sortida?
- Com es pot comprovar que la configuració anterior es correcta?
- Com es guarda la configuració de nftables en un fitxer de manera que es carregui automàticament?

Informe pràctica 2 sessió 1 i 2:

***** Introducció de l'escenari:**

En aquesta pràctica, és fonamental entendre detalladament tots els components involucrats. Per això, començarem descrivint la configuració i funcionalitats de cada element dins de l'escenari:

**** Configuració de les màquines virtuals:**

Hi hauran mínimes 2 màquines (routers) amb la intenció d'unes quantes més per:

- Router d'accés (routeracces):
Interfície eth-troncal: Connectat a Internet, configuració DHCP per obtenir una adreça IP de la xarxa troncal (x.y.z.u/m).
Interfície eth-dmz: Assignació estàtica de l'IP 10.1.10.1, connectat a la xarxa DMZ.
- Router intern (routerintern):
Interfície eth-dmz: Assignació estàtica de l'IP 10.1.10.2, connectat a la xarxa DMZ.
Interfície eth-clients: Assignació estàtica de l'IP 10.1.20.1, connectat a la xarxa de clients.
- Servidors DNS i SSH:
DNS1 i DNS2: Tots dos amb interfície eth-dmz i IPs estàtiques 10.1.10.3 i 10.1.10.4, respectivament
- Servidor Nagios (nagiosserver):
Interfície eth-servers: Assignació estàtica de l'IP 10.1.10.5.
- Monitor de Xarxa (varia segons ubicació):
Interfície eth0: Assignació estàtica de l'IP x.y.z.11 quan està connectat a la xarxa troncal.

**** Configuració de Connectivitat IP:**

Per cada màquina i servidors virtuals que implementem, es fundamental saber com es comunicaran:
- Router d'accés: Utilitza DHCP per a la seva interfície eth-troncal (dinàmica) i una adreça estàtica per a eth-dmz.
- Router intern: Adreces estàtiques per a totes les seves interfícies per a assegurar rutes fixes i control sobre la xarxa.
- Servidors i Monitor de Xarxa: Adreces estàtiques per assegurar accessibilitat constant i monitoratge eficaç.

**** Configuració de la xarxa:**

Hi hauran 3 xarxes en aquest escenari:
- Xarxa Troncal:
Actua com l'enllaç principal entre Internet i l'organització, gestionant tot el trànsit entrant i sortint.Implementa mesures robustes com firewalls i NAT per protegir els recursos interns i regular l'accés extern.
El router per defecte per als dispositius en aquesta xarxa seria el router d'accés.
Serà de tipus xarxa bridge.

- Xarxa DMZ:

Funciona com una àrea d'amortiment, allotjant serveis externs accessibles des d'Internet (per exemple, servidors web i de correu) mentre protegeix la xarxa interna. Encara que és accessible des de l'exterior, s'implementen controls estrictes per limitar el trànsit cap i des de la xarxa interna.
El router per defecte per als dispositius dins la DMZ seria el router intern, encara que també poden tenir rutes a través del router d'accés per a accés a Internet.
Serà de tipus xarxa interna.

- Xarxa de Clients:
Allotja els dispositius dels usuaris finals i proporciona accés controlat a recursos interns i connexions a Internet. Protegida per polítiques de firewall i NAT al router intern, assegura que l'accés a la xarxa sigui segur i gestiona la connexió a Internet.
El router per defecte és el router intern.
Serà de tipus xarxa interna.

**** Comunicació entre les xarxes:**
Entre les diferents xarxes, és important saber quines tenen connexió entre elles i quines no:

- De/per arribar a Internet:
El trànsit d'Internet és principalment dirigit al router d'accés i pot arribar a la DMZ per serveis específics. La xarxa de clients no té accés directe des d'Internet.

- Entre DMZ i Clients:
No hi ha comunicació directa a menys que es configurin normes específiques en el router intern per permetre cert trànsit específic per raons de serveis o administració.

- Dins de la DMZ:
Els servidors poden comunicar-se entre si segons les necessitats dels serveis que ofereixen. L'accés de la DMZ a la xarxa troncal o Internet és controlat per regles de firewall al router d'accés.

- Dins de la Xarxa de Clients:
Comunicació lliure dins la xarxa. Accés a Internet a través del router intern, amb polítiques de NAT i firewall aplicades per a seguretat.

Aquesta configuració assegura una gestió efectiva del trànsit de dades, protecció de les xarxes internes i facilita la connectivitat adequada per a cada tipus d'usuari i servei dins de l'organització.

***** Configuració dels routers:**

Per establir un entorn de xarxa amb dues màquines virtuals Debian que funcionen com a routers en un entorn VirtualBox (VB), és essencial seguir una sèrie de passos ordenats i detallats. A continuació, explquem de manera més estructurada i amb detalls ampliats el procés:

Crear una Màquina Virtual Debian o tenir una màquina base amb les especificacions més bàsiques en VirtualBox.
Una vegada configurada la primera màquina, clona aquesta per crear una segona instància. Això assegura que ambdues màquines parteixen amb una configuració de sistema idèntica.
l'assignació de Rols de les màquines serà:

- Router 1 (Router d'Accés): La primera màquina actuarà com el router d'accés.
- Router 2 (Router Intern): La màquina clonada serà configurada com el router intern.

Abans d'inicialitzar els dos routers, anar a l'apartat de Configuració i dins de Xarxes, en aquesta pàgina activar les següents interfícies pels diferents routers:

Router d'accés:
Aquest router gestionarà el trànsit entre Internet i la xarxa interna de l'organització, així com entre Internet i la xarxa DMZ.

- Adaptador 1: Xarxa Troncal

Tipus d'Adaptador: Adaptador Pont
Aquesta configuració permet que l'adaptador del router virtual s'uni directament a una xarxa física existent, és essencial per permetre que el router d'accés comunica directament amb la xarxa externa com l'Internet.
(Nom de l'Adaptador en VirtualBox serà: ent-troncal)
Direcció MAC: 08:00:27:00:00:01

- Adaptador 2: Xarxa DMZ

Tipus d'Adaptador: Xarxa interna
Nom: xarxa-dmz
Activar DHCP per assignar automàticament adreces IP dins d'aquest rang a les interfícies connectades.
Direcció MAC: 08:00:27:01:10:01

Router Intern:
Aquest router maneja la connexió i seguretat entre la xarxa DMZ i la xarxa de clients, així com el trànsit intern entre aquestes xarxes.

- Adaptador 1: Xarxa DMZ

Tipus d'Adaptador: Xarxa interna
Triarem la xarxa sota el mateix nom: xarxa-dmz
Direcció MAC: 08:00:27:01:10:02

- Adaptador 2: Xarxa Clients

Tipus d'Adaptador: Xarxa interna
Nom: xarxa-clients
Habilita DHCP per gestionar la distribució d'IPs dins aquesta xarxa.
Aquest adaptador gestiona la connexió i la traducció d'adreces per la xarxa de clients, permetent l'accés controlat a recursos més amplis i a la xarxa DMZ si es requereix.
(Nom de l'Adaptador en VirtualBox serà: clients)

Direcció MAC: 08:00:27:01:20:01

Tenint les dues màquines configurades, primer de tot serà canviar-lis els noms per diferenciar-les millor:
Anar al fitxer: /etc/hosts i també en /etc/hostname
i canviar el nom original per el router1: routeracces i el router 2: routerintern
Seguit d'un reboot per guardar els noms

Una vegada tenim les dues màquines inicalitzades, hem de mirar quin és l'estat de les seves interfícies. Actualment tindrem els noms originals com: enp0s8 o enp0s3 per les interfícies xarxa interna o bridge i sense la ip establerta per l'enunciat, només les macs implementades originalment.

Per configurar les adreces ips de les màquines segons l'enunciat, això sha de fer a través del fitxer: /etc/network/interfaces

On el router d'accés hauria de quedar com:

```
# PRIMARY eth-troncauto enp0s3
allow-hotplug enp0s3
iface enp0s3 inet dhcp

# eth-dmz
auto enp0s8
allow-hotplug enp0s8
iface enp0s8 inet static
        address 10.1.10.1
        netmask 255.255.255.240
```

I el router intern hauria de tenir per ara:

```
# eth-dmz
auto enp0s3
iface enp0s3 inet static
        address 10.1.10.2
        netmask 255.255.255.240

# Clients
auto enp0s8
iface enp0s8 inet static
        address 10.1.20.1
        netmask 255.255.255.0
```

Ara tenint la configuració mínima de les interfícies, hem de canviar-lis el nom perquè aquest es corresponguin als noms que l'enunciat estan donades.

Per fer això s'haurà de crear un nou fitxer de configuració d'aquella interfície
Per exemple en el router d'accés per la enp0s3(xarxa troncal) serà en el fitxer:

/etc/systemd/network/10-enp0s3-net.link

```
[Match]
OriginalName=enp0s3

[Link]
Name=eth-troncal
```

Pel router d'accés per la enp0s3 (xarxa dmz) serà el fitxer:
/etc/systemd/network/10-enp0s8-net.link

```
[Match]
OriginalName=enp0s8

[Link]
Name=eth-dmz
```

Pel router intern per la enp0s3 (xarxa dmz) serà el fitxer:
/etc/systemd/network/10-enp0s3-net.link

```
[Match]
OriginalName=enp0s3

[Link]
Name=eth-dmz
```

Pel router intern per la enp0s8 (xarxa clients) serà el fitxer:
/etc/systemd/network/10-enp0s8-net.link

```
[Match]
OriginalName=enp0s8

[Link]
Name=eth-clients
```

Ara si es fa un reboot els canvis es veuran si es fa un : ip a On es pot veure el canvi del nom de la interfície, per exemple en el router d'accés:

```
..
2: eth-troncal: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
   link/ether 08:00:27:00:00:01 brd ff:ff:ff:ff:ff:ff
   altname enp0s3
…
```

Ara també s'haurà d'actualitzar el fitxer de /etc/network/interfaces perquè quadrin els noms.

El fitxer del router d'accés serà:

```
# The loopback network interface
auto lo
iface lo inet loopback
```

```
# eth-troncal
allow-hotplug eth-troncal
iface eth-troncal inet dhcp

# eth-dmz
allow-hotplug eth-dmz
iface eth-dmz inet static
        address 10.1.10.1
        netmask 255.255.255.240
```

El fitxer del router intern serà:

```
# The loopback network interface
auto lo
iface lo inet loopback

# eth-dmz
allow-hotplug eth-dmz
iface eth-dmz inet static
        address 10.1.10.2

# eth-clients
allow-hotplug eth-clients
iface eth-clients inet static
        address 10.1.20.1
        netmask 255.255.255.0
```

Per guardar els canvis executar: systemctl restart networking.service
Seguidament fer un reboot per aplicar tots els canvis fets anteriorment i que quan el sistema es reinici tingui tots els canvis aplicats.

Una vegada fets aquests passos, podem tornar a fer un: ip a per veure verificar que les ips configurades i els noms de les interfícies han estat implementat correctament:

On el router d'accés hauria de quedar com:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth-troncal: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:00:00:01 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 192.168.0.21/24 brd 192.168.0.255 scope global dynamic eth-troncal
```

```
    valid_lft 86396sec preferred_lft 86396sec
  inet6 fe80::a00:27ff:fe00:1/64 scope link
    valid_lft forever preferred_lft forever
3: eth-dmz: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
  link/ether 08:00:27:01:10:01 brd ff:ff:ff:ff:ff:ff
  altname enp0s8
  inet 10.1.10.1/28 brd 10.1.10.15 scope global eth-dmz
    valid_lft forever preferred_lft forever
  inet6 fe80::a00:27ff:fe01:1001/64 scope link
    valid_lft forever preferred_lft forever
```

On el Router intern hauria de quedar com:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth-dmz: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
  link/ether 08:00:27:01:10:02 brd ff:ff:ff:ff:ff:ff
  altname enp0s3
  inet 10.1.10.2/28 brd 10.1.10.15 scope global eth-dmz
    valid_lft forever preferred_lft forever
  inet6 fe80::a00:27ff:fe01:1002/64 scope link
    valid_lft forever preferred_lft forever
3: eth-clients: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
  link/ether 08:00:27:01:20:01 brd ff:ff:ff:ff:ff:ff
  altname enp0s8
  inet 10.1.20.1/24 brd 10.1.20.255 scope global eth-clients
    valid_lft forever preferred_lft forever
  inet6 fe80::a00:27ff:fe01:2001/64 scope link
    valid_lft forever preferred_lft forever
```

Amb aquesta configuració es pot verificar l'estat de l'escenari actual:
Comprovant que des del router d'accés (10.1.10.1) inicalment, quan el router intern no està creat, no pot connectar-se a ell (10.1.10.2).
Però una vegada s'ha configurat el router intern, si es pot fer un ping (10.1.10.2), fent servir així la xarxa DMZ i també cap a internet, fent un ping a google.com, utilitzant la xarxa troncal.
També es pot comprovar que des del router intern (10.1.10.2) es pot fer un ping al router d'accés (10.1.10.1) ja que estan sota la mateixa xarxa dmz, però no cap a internet, ja que encara no té cap ruta per accedir a la xarxa troncal.

**** Creació del monitor**

Per configurar una màquina virtual bàsica a VirtualBox que funcioni com a monitor de xarxa, s'ha de fer inicialment com s'ha fet els dos routers.
Primer canviar els noms de la màquina en els fitxers per tenir el nom de: monitor, en el fitxer de /etc/hosts i també en /etc/hostname
Fer un reboot per guardar els canvis.

Des de una màquina base, configurarem un monitor que tingui accés a les tres xarxes, per fer això, des de la configuració posarem que tindrem 3 adaptadors que anirem activan o desactivan depenen de la xarxa on ens volem situar:
1. Adaptador bridge: xarxa troncal: Aquest adaptador està configurat per connectar-se a la xarxa principal o troncal, i està establert per obtenir una adreça IP dinàmicament via DHCP. És el punt de connexió principal de la màquina amb la xarxa més àmplia o amb Internet. Aquesta configuració permet a la màquina comunicar-se amb altres dispositius fora de les xarxes internes definides i gestionar el trànsit entrant i sortint.
Amb
2. Adaptador xarxa interna: xarxa dmz: Configurat amb una adreça IP estàtica, aquest adaptador connecta la màquina a una zona desmilitaritzada (DMZ). Les DMZ són utilitzades per tenir serveis que necessiten ser accessibles des de l'Internet extern però aïllats de la xarxa interna crítica per raons de seguretat.

3. Adaptador xarxa interna: xarxa client: També configurat amb una adreça IP estàtica, aquest adaptador serveix la xarxa interna de clients. Aquest segment de la xarxa és on es connecten els dispositius d'usuari final, com ordinadors de treballadors, dispositius mòbils, i altres equips que requereixen accés a recursos compartits internament però que no necessiten exposició directa a la xarxa més àmplia o a Internet.

Posant a tots els adaptadors la mac: 08:00:27:01:00:11

Una vegada iniciem la màquina, podem veure que cal configurar les ips per les diferents interfícies, ja que actualment només tenen la mac configurada:
/etc/network/interfaces

```
# The loopback network interface
auto lo
iface lo inet loopback

# Bridge - XARXA TRONCAL
allow-hotplug enp0s3
iface enp0s3 inet dhcp

#Interna - XARXA DMZ
allow-hotplug enp0s8
iface enp0s8 inet static
        address 10.1.10.11
        netmask 255.255.255.240
        network 10.1.10.0
```

```
        gateway 10.1.10.1

#Interna -XARXA CLIENT
allow-hotplug enp0s9
iface enp0s9 inet static
        address 10.1.20.11
        netmask 255.255.255.0
        network 10.1.20.0
        gateway 10.1.20.1
```

Xarxa troncal (enp0s3)
Amb mode DHCP, aquesta interfície connecta al router amb Internet o la xarxa principal externa. Obtenint una adreça IP automàticament via DHCP, facilita l'accés ampli sense necessitat de configuració estàtica.
Xarxa DMZ (enp0s8)
Amb mode Estàtic, l'adreça IP: 10.1.10.11, amb màscara de Subxarxa: 255.255.255.240 i la passarel·la: 10.1.10.1, sent la de la xarxa dmz. Serveix com a pont entre Internet i la xarxa interna, ideal per allotjar serveis que necessiten ser accessibles externament però aïllats de la xarxa corporativa interna.
Xarxa de Clients (enp0s9)
Amb mode Estàtic, l'adreça IP: 10.1.20.11, la màscara de Subxarxa: 255.255.255.0 i la passarel·la: 10.1.20.1. Utilitzada per connectar dispositius de clients dins de l'organització, proporcionant una configuració fixa per a gestió fàcil i seguretat reforçada.
*(Futurament es donarà la ip amb DHCP quan el router intern tingui aquest servei)

Tenint ara configurat totes les ips, podrem anar canviant de xarxa activant i desactivant les diferents interfícies.
Per poder canviar el nom del monitor per cada xarxa diferent, hem fet un script que detecta en quina xarxa està i actualitza el nom de la màquina: nommonitor.sh
Donar-li permisos d'execució amb: chmod +x nommonitor.sh

```
#!/bin/bash
# Obté l'adreça IP de la interfície activa
IP=$(ip -4 addr show scope global | grep inet | head -n1 | awk '{print $2}' | cut -d'/' -f1)

# Defineix les xarxes i els noms associats
if [[ $IP == 10.1.10.* ]]; then
   NEWNAME="monitordmz"
elif [[ $IP == 10.1.20.* ]]; then
   NEWNAME="monitorclients"
else
   NEWNAME="monitoradmin"
fi
# Obté el nom actual del host
CURRENTNAME=$(hostname)
```

```
# Comprova si el nou nom és diferent del nom actual
if [[ $CURRENTNAME != $NEWNAME ]]; then
   echo $NEWNAME | tee /etc/hostname
   hostname $NEWNAME
   echo "Canviat el nom de la màquina i reiniciant..."
   reboot
else
     echo "El nom de la màquina ja està configurat correctament. No es necessita reinici."
fi
```

Per executar-lo només cal fer: ./nommonitor.sh
Obté la ip de la màquina actual, recuperant la primera adreça ipv4 de la primera interfície activa de la màquina, excluint la adreça de loopback i les adreces globals. Depenen de la ip que trobi donarà un nom o un altre al monitor. Aquest nou nom el compara amb el nom actual del host de la màquina, si aquest és diferent canviarà el nom de host del sistema i farà un reboot per guardar els canvis del nom, però si el nom del monitor és el mateix que la xarxa actual no executarà res.

Amb aquesta configuració es pot verificar l'estat de l'escenari actual:
Xarxa Troncal:
Ping a Google.com Confirma que la màquina té accés a Internet i que la connexió és estable i ràpida.
Ping a 10.1.10.1 (Gateway DMZ): Indica que no hi ha connectivitat amb l'adreça IP del gateway de la Xarxa DMZ des d'aquesta màquina.Des de internet no ha de ser possible entrar en la xarxa dmz.
Ping a 10.1.20.1 (Gateway Clients): Indica que no hi ha connectivitat amb l'adreça IP del gateway de la Xarxa de Clients des d'aquesta màquina.Des de internet no ha de ser possible entrar en la xarx dels clients.

Xarxa DMZ:
Ping a 10.1.10.1 (Propi Gateway DMZ): Confirma la connectivitat dins de la pròpia xarxa DMZ.
Ping a 10.1.20.1 (Gateway Clients): Indica connectivitat amb el gateway de la Xarxa de Clients
Ping a Google.com:Encara no hi ha connexió a Internet (abans de la configuració de la NAT)

Xarxa Clients:
Ping a 10.1.10.1 (Gateway DMZ): Confirma la connectivitat amb el gateway de la Xarxa DMZ, indicant una bona connexió entre aquestes dues xarxes.
Ping a 10.1.20.1 (Propi Gateway Clients): Confirma la connectivitat dins de la pròpia xarxa de Clients
Ping a Google.com: Encara no hi ha connexió a Internet (abans de la configuració de la NAT)

Fitxers involucrats:
- /etc/hosts i /etc/hostnames

Per modificar els noms de les màquines virtuals
- /etc/network/interfaces
Per tota la configuració feta pels adaptadors de els diferents xarxes
- /etc/systemd/network/10-enp0s3-net.link
Per guardar els canvis dels noms de les interfícies
- nommonitor.sh
Script creat per canviar el nom del monitor per la xarxa que estigui connectat

Fitxers d'evidència:

configuració router d'accés:	1-1-config-routeracces.txt
configuració router intern:	1-1-config-routerintern.txt
configuració monitor:	1-1-config-monitor.txt

Es poden veure els resultats de l'execució de les explicacions anteriors
Al final de la configuració dels routers hi ha la verificació de la connexió entre routers amb format ping.
Al final de la configuració del monitor hi ha la verificació de la connexió entre routers amb format ping en totes les xarxes troncal amb el monitoradmin, xarxa dmz amb monitordmz i xarxa clients amb monitorclients.

***** Configuració de l'encaminament:**

Una vegada hem configurat inicialment els routers, hem d'establir les seves rutes d'encaminament, siguin les predefinides o les que enllacen els dos routers.

Primer de tot, per configurar una màquina com a router, és imprescindible que tinguin la configuració de reenviament de paquets entre diferents xarxes, que és essencial per a les funcions de routing.
Per fer aixo s'ha de anar al fitxer de: /etc/sysctl.conf
i descomentar la següent línea:

Uncomment the next line to enable packet forwarding for IPv4
-- > net.ipv4.ip_forward=1

Per guardar aquesta configuració s'ha d'executar la comanda per carregar les configuracions del sistema especificades en els fitxers de configuració de sysctl: sysctl -p

A partir d'aquí ara es pot configurar l'encaminament per cada router.
Per començar a fer això, hem de saber quines rutes necessitem i quines rutes ja estan implementades.
Podem mirar les rutes executant: ip route show

Pel router d'accés tenim les següents rutes implementades:

default via 192.168.0.1 dev eth-troncal
10.1.10.0/28 dev eth-dmz proto kernel scope link src 10.1.10.1

192.168.0.0/24 dev eth-troncal proto kernel scope link src 192.168.0.21

1. Ruta per defecte: Trafic a xarxes desconegudes enviat a 192.168.0.1 utilitzant l'interficie eth-troncal que té accés a internet.
2. Ruta per la xarxa DMZ: gestiona el trànsit dins de la xarxa dmz (10.1.10.0/28) utilitzant l'interficie eth-dmz amb l'adreça IP 10.1.10.1 com a font.
3. Ruta per la xarxa local: gestiona el trànsit dins de la xarxa local (192.168.0.0/24) a través de eth-troncal amb IP 192.168.1.21.

Falta una ruta específica que dirigeixi el trànsit des del router d'accés al router intern utilitzant la xarxa DMZ, per permetre una comunicació eficaç entre els dos routers i per gestionar correctament el trànsit cap a la xarxa de clients si aquest passa a través del router intern.

Pel router intern tenim les següents rutes implementades:

10.1.10.0/28 dev eth-dmz proto kernel scope link src 10.1.10.2
10.1.20.0/24 dev eth-clients proto kernel scope link src 10.1.20.1

1. Ruta per la xarxa DMZ: gestiona el trànsit dins de la xarxa dmz (10.1.10.0/28) utilitzant l'interficie eth-dmz amb l'adreça IP 10.1.10.2 com a font.
2. Ruta per la xarxa Clients: gestiona el trànsit dins de la xarxa de clients (10.1.20.0/24) , utilitzant l'interfície eth-clients amb l'adreça IP 10.1.20.1 com a font.

Falta una ruta per defecte en el router intern, la qual és essencial per permetre que el router intern envii trànsit destinat a adreces fora de les seves xarxes directament connectades (com a Internet o altres xarxes en l'organització que no estiguin dins de la DMZ o la xarxa de clients)

sudo ip route add default via 10.1.10.1 dev eth-dmz

Per fer les rutes addicionals es podria executar una comanda com aquesta:

sudo ip route add 10.1.20.0/24 via 10.1.10.2 dev eth-dmz

Però la ruta no es guardaria en cap fitxer de configuració i seria una ruta temporal. Aquesta ruta seria borrada en fer un reboot o un reinici del servei de xarxa, només és útil per a proves o configuracions temporals.

Però si es vol fer rutes persistents s'ha de modificar el fitxer d'interfícies, aquest gestiona les interfícies de xarxa i es pot afegir la ruta directament al fitxer de configuració de la interfície:

En el router d'accés seria així el fitxer /etc/network/interfaces:

```
# The loopback network interface
auto lo
iface lo inet loopback

# eth-troncal
allow-hotplug eth-troncal
iface eth-troncal inet dhcp

# eth-dmz
```

```
allow-hotplug eth-dmz
iface eth-dmz inet static
        address 10.1.10.1
        netmask 255.255.255.240
        post-up /usr/sbin/ip route add 10.1.20.0/24 via 10.1.10.2 dev eth-dmz
```

La lína post-up indica que el comandament següent s'ha de realitzar just després que l'interfície de xarxa s'hagi engegat i estigui en línia I /usr/sbin/ip route add: Aquest és el camí complet a l'eina ip i l'acció que realitza és afegir una nova ruta a la taula d'encaminament del sistema.
10.1.20.0/24: Aquest és el bloc de xarxa de destinació per a la ruta que s'està afegint. Totes les adreces IP dins d'aquest rang seran afectades per aquesta ruta.
via 10.1.10.2: Això especifica la passarel·la a través de la qual el trànsit hauria de passar per arribar a la xarxa de destinació. És la IP de l'interfície o dispositiu que manejarà el trànsit cap a aquesta xarxa.
dev eth-dmz: Especifica l'interfície de xarxa a través de la qual s'ha d'encaminar el trànsit, en aquest cas, eth-dmz.

En el router intern seria així el fitxer /etc/network/interfaces: :

```
#loopback
auto lo
iface lo inet loopback

#eth-dmz
allow-hotplug eth-dmz
iface eth-dmz inet static
        address 10.1.10.2
        netmask 255.255.255.240
        gateway 10.1.10.1

#eth-clients
allow-hotplug eth-clients
iface eth-clients inet static
        address 10.1.20.1
        netmask 255.255.255.0
```

La lína gateway 10.1.10.1 dev eth-dmz s'utilitza per afegir una ruta per defecte a la taula d'encaminament, especificament quan l'interfície eth-dmz s'activa. Això significa que tot el trànsit de xarxa sense una ruta específica serà enviat a través de l'interfície eth-dmz cap a la passarel·la 10.1.10.1. Aquesta configuració s'aplica automàticament cada vegada que l'interfície es posa en línia, assegurant que el router pot comunicar-se amb xarxes externes a través d'aquesta passarel·la.

Per guardar el canvi executar: systemctl restart networking.service
Ara les taules d'encaminament serien:

Pel router d'accés:

default via 192.168.0.1 dev eth-troncal
10.1.10.0/28 dev eth-dmz proto kernel scope link src 10.1.10.1
10.1.20.0/24 via 10.1.10.2 dev eth-dmz
192.168.0.0/24 dev eth-troncal proto kernel scope link src 192.168.0.21

Pel router intern:

default via 10.1.10.1 dev eth-dmz
10.1.10.0/28 dev eth-dmz proto kernel scope link src 10.1.10.2
10.1.20.0/24 dev eth-clients proto kernel scope link src 10.1.20.1

Amb aquesta configuració es pot verificar l'estat de l'escenari actual:
Comprovant que des del router d'accés (10.1.10.1) es pot fer un ping al router intern (10.1.10.2), fent servir així la xarxa DMZ i també cap a internet, fent un ping a google.com, utilitzant la xarxa troncal i ara també cap al router intern (10.1.20.1).
També es pot comprovar que des del router intern es pot fer un ping al router d'accés (10.1.10.1) ja que estan sota la mateixa xarxa dmz i també en la xarxa de clients (10.1.20.1) però encara no cap a internet , igualment que tingui una ruta per la xarxa troncal, encara s'ha de configurar la NAT dels dos routers.

Fitxers involucrats:
- /etc/sysctl.conf
Modificació de la configuració de reenviament de paquets ip4
- /etc/network/interfaces
Per posar les rutes persistens en els dos routers

Fitxers d'evidència:

Router d'accés: 1-2-encaminament-routeracces.txt
Router intern: 1-2-encaminament-routerintern.txt

Es poden veure els resultats de l'execució de les explicacions anteriors
Al final de la configuració dels routers hi ha la verificació de la connexió entre routers amb format ping i les taules d'encaminament.

***** Configuració de la NAT**

La NAT (Network Address Translation) és un mètode utilitzat per mapejar una adreça IP i port d'una xarxa a una altra adreça i port. Aquesta tècnica és comunament utilitzada per permetre que múltiples dispositius en una xarxa privada accedeixin a Internet utilitzant una única adreça IP pública. La NAT ajuda a conservar les adreces IP (que són limitades) i augmenta la seguretat amagant les adreces IP internes del món exterior.
En el nostre cas la farem servir per donar connexió a internet a tots els clients, això serà des de la xarxa troncal on hi ha l'accés, passant per xarxa dmz, i arribant a la xarxa interna dels clients.

Per configurar la Nat, s'utilitzarà la configuració de les nftables, una eina configurar i gestionar les taules de filtratge de paquets. Aquesta part es farà principalment en el router d'accés, ja que serà aquest el que ha de gestionar l'accés a internet.

En el router d'accés crear una taula nat per poder inserir les noves normes nat, això es farà executant: nft add table ip nat

Executant la 'add chain ip nat postrouting { type nat hook postrouting priority 100\; }'
Afegeix una cadena anomenada postrouting a la taula nat. Aquesta cadena és de tipus NAT i s'enganxa a l'esdeveniment postrouting, que és un punt d'ancoratge utilitzat per processar paquets després que hagin estat rutats. Aquesta cadena té una prioritat de 100, que determina l'ordre de processament respecte a altres cadenes.

Executant la add rule ip nat postrouting oifname "eth-troncal" masquerade
Afegeix una regla a la cadena postrouting que aplica la tècnica de masquerade a tot el tràfic que surt per la interfície eth-troncal. Masquerade és una forma específica de NAT que amaga les adreces IP d'origen dels paquets sortints, substituint-les per l'adreça IP de la interfície per la qual els paquets surten. Aquesta tècnica és útil per xarxes on l'adreça IP de la interfície pot canviar dinàmicament, com en connexions DHCP que tindran els clients.

Copiar la configuració creada en el fitxer de configuració:
nft list ruleset > /etc/nftables.conf

Per mirar si s'han inserit correctament les normes executar: nft list ruleset
o des de cat /etc/nftables.conf
Per veure totes les taules, cadenes i regles configurades:

```
table inet filter {
	chain input {
		type filter hook input priority filter; policy accept;
	}

	chain forward {
		type filter hook forward priority filter; policy accept;
	}

	chain output {
		type filter hook output priority filter; policy accept;
	}
}
table ip nat {
	chain postrouting {
		type nat hook postrouting priority srcnat; policy accept;
		oifname "eth-troncal" masquerade
	}
}
```

Per aplicar els canvis executar : nft -f /etc/nftables.conf

Per fer que s'iniciin automàticament en l'arrencada del sistema i després que inicien el servei de nftables, executar en el router d'accés:
systemctl enable nftables
systemctl start nftables

Una vegada fet tot això, es pot veure l'estat actual del servei nftables executant: systemctl status nftables

● nftables.service - nftables
Loaded: loaded (/lib/systemd/system/nftables.service; enabled; preset: enabled)
Active: active (exited) since Fri 2024-05-03 12:45:37 CEST; 5s ago
Docs: man:nft(8)
http://wiki.nftables.org
Process: 597 ExecStart=/usr/sbin/nft -f /etc/nftables.conf (code=exited, status=0/SUCCESS)
Main PID: 597 (code=exited, status=0/SUCCESS)
CPU: 6ms

may 03 12:45:37 routeracces systemd[1]: Starting nftables.service - nftables...
may 03 12:45:37 routeracces systemd[1]: Finished nftables.service - nftables.

Pel router intern, s'han de canviar vàries coses per poder configurar la connexió amb el router d'accés:
Verificar que en el fitxer de la configuració de les interfícies utilitzi el gateway de la xarxa dmz. On podem modificar la línia de ruta default implementada anteriorment, pel gateway de la xarxa dmz, que farà com si fos la default.

cat /etc/network/interfaces
…
eth-clients
allow-hotplug eth-clients
iface eth-clients inet static
address 10.1.20.1
netmask 255.255.255.0

Les rutes d'encaminament de: ip route show no haurien de canviar.

S'ha de mirar el fitxer de configuració de resolv.conf per veure quins nameservers utilitza, i modificar-lo perquè utilitzi el servidor de la xarxa dmz:
cat /etc/resolv.conf
nameserver 10.1.10.1
nameserver 192.168.1.1

nameserver 212.166.132.192
nameserver 212.166.132.96

1. nameserver 10.1.10.1: Aquesta adreça correspon al servidor DNS dins de la xarxa DMZ. El router intern utilitzarà aquest servidor per resoldre noms de domini.
2. nameserver 192.168.1.1: Aquest és un altre servidor DNS, el de la xarxa troncal, que també proporciona serveis DNS. Pot ser utilitzat com a alternativa o backup si el primer servidor DNS no respon.
3. nameserver 212.166.132.192 i nameserver 212.166.132.96: Aquests són servidors DNS externs, originals de virtualbox. Són utilitzats pel router intern per resoldre noms de domini quan els servidors DNS més propers o interns fallen o no estan disponibles.

Amb aquesta configuració es pot verificar l'estat de l'escenari actual:
Router d'Accés:
- Xarxa Troncal: (ping a google)
  Ping a 142.250.184.14: Èxit, amb 2 paquets transmesos i rebuts.
- Xarxa DMZ del router intern:
  Ping a 10.1.10.2: Èxit, amb 2 paquets transmesos i rebuts.
- Xarxa Clients del router intern:
  Ping a 10.1.20.1: Èxit, amb 2 paquets transmesos i rebuts.

Router Intern:
- Xarxa Troncal: (ping a google)
  Ping a 142.250.201.78: Èxit, amb 2 paquets transmesos i rebuts
- Xarxa DMZ del router d'accés:
  Ping a 10.1.10.1: Èxit, amb 2 paquets transmesos i rebuts.
- Xarxa Troncal: (especificament la xarxa del router d'accés)
  Ping a 192.168.1.26:Èxit, amb 2 paquets transmesos i rebuts

Fitxers involucrats:
- /etc/nftables.conf
Per la configuració i visualització de les normes i taules nat
- /etc/network/interfaces
Per modificar la gateway default el router intern
- /etc/resolv.conf
Per modificar els servidors dns del router intern

Fitxers d'evidència:
  configuració router d'accés: 1-3-nat-routeracces.txt
  configuració router intern: 1-3-nat-routerintern.txt

Es poden veure els resultats de l'execució de les explicacions anteriors
Al final de la configuració dels routers hi ha la verificació de la connexió entre routers amb format ping i les normes del es nft tables.

***** Configuració de SSH i DNS**

**** Servei SSH:**

SSH, que significa Secure Shell, és un protocol de xarxa que permet la comunicació segura entre dos dispositius informàtics a través d'una xarxa no segura. Utilitzat comúment per a l'administració remota de sistemes, SSH proporciona un mètode segur per executar comandaments en una màquina remota i per moure fitxers d'un sistema a un altre.

Per tenir ssh en els dos routers, el que hem de fer és instalar-nos els paquets necessaris pel seu servei, executant:
Per actualitzar la màquina: apt update
Per descargarnos el paquet de servidor ssh: apt install openssh-server

Per els monitors fer el mateix:
Per actualitzar la màquina: apt update
Per descargarnos el paquet de client ssh: apt install openssh-client

Per la mínima configuració del servidor ssh en els dos routers, es poden modificar vàries línies del fitxer de configuració de ssh, en aquest descomentem es següents línies:
/etc/ssh/sshd_config

…
PermitRootLogin no
…
PasswordAuthentication yes
…

Altres configuracions de seguretat, les aplicarem des del tallafocs que farem més endavant.
Per guardar els canvis reiniciar el servei ssh: systemctl restart sshd

I per mirar l'estat del servidor executar: systemctl status sshd
Que sortirà : " Active (running) " si aquest ha estat configurat correctament

Per la mínima configuració del monitor, el ssh client, podem modificar el mateix fitxer descomentant les següents línies:
/etc/ssh/sshd_config

…
PasswordAuthentication yes
…

Per deixar que s'entri utilitzant la contrasenya per les ssh.

Ara tenint una mínima configuració en els routers fent de servidors i en el monitor, podem mirar si es poden fer les connexions per cada xarxa en cada router.

Per cada xarxa s'ha verificat que:

*** Xarxa troncal:**

Router d'Accés:
- Xarxa Troncal:
  Ping a 192.168.1.26: Èxit, amb 2 paquets transmesos i rebuts, mostrant una baixa latència.
  SSH a 192.168.1.26: Connexió SSH exitosa. L'usuari entel va accedir, va navegar pel directori /home i va listar els continguts abans de tancar la sessió.
- Xarxa DMZ:
  Ping a 10.1.10.1: No es proporciona resultat del ping, indicant que no hi ha resposta
  SSH a 10.1.10.1: No hi ha resultat del ping, indicant que no hi ha resposta i que internet no té accés a la xarxa interna.

Router Intern:
- Xarxa DMZ:
  Ping a 10.1.10.2: No es proporciona resultat del ping, indicant que no hi ha resposta
  SSH a 10.1.10.2: No hi ha resultat del ping, indicant que no hi ha resposta i que internet no té accés a la xarxa interna.
- Xarxa Clients:
  Ping a 10.1.20.1: No es proporciona resultat del ping, indicant que no hi ha resposta
  SSH a 10.1.20.1: No hi ha resultat del ping, indicant que no hi ha resposta i que internet no té accés a la xarxa interna.

*** Xarxa dmz:**

Router d'Accés:
- Xarxa Troncal:
  Ping a 192.168.1.26: Èxit, indicant bona connectivitat.
  SSH a 192.168.1.26: Connexió SSH exitosa, mostrant que l'usuari entel pot accedir i navegar pel directori /home al mateix dispositiu que actua com a router d'accés.
- Xarxa DMZ: (xarxa del monitor)
  Ping a 10.1.10.1: Èxit, indicant bona connectivitat.
  SSH a 10.1.10.1: Connexió SSH exitosa, mostrant que l'usuari entel pot accedir i navegar pel directori /home.

Router Intern:
- Xarxa DMZ: (xarxa del monitor)
  Ping a 10.1.10.2: Èxit, indicant bona connectivitat.
  SSH a 10.1.10.2: Connexió SSH exitosa, amb accés i navegació pel directori /home per l'usuari entel.
- Xarxa de Clients:
  Ping a 10.1.20.1: Èxit, indicant bona connectivitat.
  SSH a 10.1.20.1: No s'ha proporcionat informació sobre la prova SSH en aquesta adreça, però l'èxit en el ping indica que hi ha connectivitat.

Usuari Root:

SSH com a root a 10.1.10.1 i 10.1.10.2: En ambdós casos, es denega l'accés, mostrant un missatge de "Permission denied". Això indica que l'accés com a root està desactivat.

*** Xarxa clients:**

Router d'Accés
- Xarxa Troncal:
    Ping a 192.168.1.26: Èxit, 2 paquets transmesos i rebuts.
    SSH a 192.168.1.26: Connexió establerta exitosament. L'usuari entel es va connectar, va navegar per /home, i va veure el contingut del directori abans de tancar la sessió.
    Router Intern
- Xarxa DMZ:
    Ping a 10.1.10.1: Èxit, 2 paquets transmesos i rebuts.
    SSH a 10.1.10.1: Connexió establerta exitosament. L'usuari entel es va connectar, va navegar per /home, i va veure el contingut del directori abans de tancar la sessió.

Router Intern:
- Xarxa DMZ:
    Ping a 10.1.10.2: Èxit, 2 paquets transmesos i rebuts.
    SSH a 10.1.10.2: Connexió establerta exitosament. L'usuari entel es va connectar, va navegar per /home, i va veure el contingut del directori abans de tancar la sessió.
- Xarxa Clients: (xarxa del monitor)
    Ping a 10.1.20.1: Èxit, 2 paquets transmesos i rebuts.
    SSH a 10.1.20.1: Connexió establerta exitosament. L'usuari entel es va connectar, va navegar per /home, i va veure el contingut del directori abans de tancar la sessió.

Usuari root:
    SSH com a root a 10.1.20.1: Connexió denegada, per restriccions de política de seguretat que impedeixen l'accés directe com a root.

    **** Servei DNS:**

Un servidor DNS (Domain Name System) és un component essencial de la infraestructura d'Internet que tradueix els números de domini llegibles per humans en adreces IP numèriques, i viceversa. Aquest procés es coneix com a resolució de números.
El servidor DNS funciona com un directori telefònic d' Internet, mantenint una base de dades distribuïda de noms de domini i les seves adreces IP corresponents. Quan realitzeu una consulta DNS, el vostre dispositiu envia una sol·licitud al servidor DNS especificat, que cerca a la base de dades i retorna l'adreça IP associada amb el nom de domini sol·licitat.

Per fer les comprovacions del servidor DNS, el que podem utilitzar es les eines de : dig i tcpdump.
Amb comanda dig retorna la la direcció IP associada amb el nom de domini consultat, en aquest cas, google.com, així que ho comprovem des dels diferents monitors:

- Des del monitoradmin (xarxa troncal): S'ha obtingut una resposta amb la IP d'enregistrament associada al nom de domini google.com. (status: NONERROR)
IP obtinguda per a google.com: 142.250.201.78
- Des del monitordmz (xarxa DMZ): Igual que abans, s'ha obtingut la IP associada a google.com. (status: NONERROR)IP obtinguda per a google.com: 142.250.200.78

- Des del monitorclients (xarxa de clients): La resposta també ha retornat la IP corresponent a google.com. (status: NONERROR)IP obtinguda per a google.com: 142.250.200.78

La distribució de les respostes entre els servidors DNS de la DMZ mostra una alternança entre les IPs obtingudes per a la mateixa consulta google.com. Això suggereix que els clients que fan peticions DNS poden ser dirigits a diferents servidors DNS de la DMZ, probablement com a part d'un mecanisme de balanceig de càrrega. Això es confirma perquè les respostes mostren adreces IP diferents (142.250.201.78 i 142.250.200.78) però vàlides per al mateix domini google.com.

I la comprovació utilitzant el tcpdump, el que fem es per capturar el tràfic DNS (del port 53) a la interfície eth-dmz i guardar-lo en un fitxer pcap anomenat sortidadns1.pcap, executant:

```
tcpdump -i eth-dmz port 53 -w sortidadns1.pcap
```

Tenint la terminal oberta podem anar fent digs entre els diferents monitors o el router intern, i una vegada acabem l'execució del tcpdump, es poden veure els diferents paquets que s'han capturat amb el tràfic de DNS.

La captura del tcpdump és el fitxer: 1-4-dns-wiresharkpaquets.txt

Fitxers involucrats:
- /etc/ssh/sshd_config
Per la configuració del servei ssh
- /etc/ssh/sshd_config
Per la configuració del client ssh

Fitxers d'evidència:

Router d'accés: 1-4-ssh-routeracces.txt
Router intern: 1-4-ssh-routerintern.txt
Configuració monitor: 1-4-ssh-configmonitor.txt

Verificació xarxa troncal:	1-4-ssh-monitortroncal.txt
Verificació xarxa dmz:	1-4-ssh-monitordmz.txt
Verificació xarxa clients:	1-4-shh-monitorclients.txt
Verificació dns:	1-4-dns-monitors.txt
fitxer tcpdump	1-4-dns-wiresharkpaquets.txt

Es poden veure els resultats de l'execució de les explicacions anteriors
Al final de la configuració dels routers hi ha la verificació de la connexió entre routers amb format ping.

***** Configuració del tallafocs**

Un tallafocs (o firewall en anglès) és una part crítica de la infraestructura de seguretat d'una xarxa, que actua com una barrera entre una xarxa interna i el món exterior. El seu objectiu principal és protegir els dispositius de la xarxa interna contra accés no autoritzat o tràfic maliciós. Això s'aconsegueix mitjançant la imposició de polítiques de seguretat que controlen quin tràfic està permès entrar o sortir de la xarxa.

Els tallafocs poden operar en diferents capes del model OSI, des de la capa de xarxa fins a la capa d'aplicació, i poden ser tant de maquinari com de programari. Un tallafocs pot:

- Bloquejar/Permetre Tràfic Basat en Adreces IP: Determina si el tràfic des de o cap a certes adreces IP està permès.
- Filtrar Ports i Protocols: Permet o bloqueja el tràfic basat en ports TCP/UDP i protocols.
- Inspecció d'Estat: Monitoritza l'estat de les connexions actives per assegurar que només les respostes a les sol·licituds internes són permeses.
- Funcionalitats Avançades: Inclou la inspecció profunda de paquets (DPI), prevenció d'intrusions, i més.

Els tallafocs es configuren per filtrar paquets d'acord amb les comunicacions que es permeten mitjançant la definició de regles específiques que determinen quin tipus de trànsit es permet passar a través del tallafoc i quin tipus es bloqueja.

Per balancejar la càrrega entre dos servidors amb un tallafocs, es poden utilitzar tècniques com el NAT (Network Address Translation) o el servei de balanceig de càrrega integrat en alguns tallafocs. En el cas del NAT, es pot configurar una regla que redireccioni el trànsit entrant a una determinada adreça IP i port cap a una de les adreces IP dels servidors amb una relació de round-robin, assegurant-se que el trànsit s'equilibri entre ells.
Per redirigir un port amb un tallafocs, es pot utilitzar la tècnica de reenviament de ports. Això es fa creant una regla que especifica quin port d'origen i destí s'ha de redirigir i cap a quina adreça IP i port s'ha de reenviar. Això permet redirigir el trànsit entrant d'un port específic cap a una altra adreça IP i port, útil per redirigir serveis o aplicacions a diferents servidors dins de la xarxa.

Per redirigir el trànsit d'un port específic cap a una altra adreça IP i port utilitzant un tallafocs, pots utilitzar la següent comanda de nftables com a exemple:

```
nft add rule inet filter prerouting tcp dport 80 dnat to 192.168.1.2:8080
```

Aquesta comanda redirigirà tot el trànsit TCP que arribi al port 80 cap a l'adreça IP 192.168.1.2 al port 8080. Això pot ser útil, per exemple, si vols redirigir les peticions HTTP (port 80) d'un servidor a un altre servidor o servei que s'estigui executant a un port diferent (com ara un servidor web que escolta al port 8080).

La configuració del tallafoc implica la definició de les següents característiques:

- Regles de filtratge: Les regles defineixen les condicions específiques que els paquets de dades han de complir per ser acceptats o rebutjats pel tallafoc. Aquestes regles poden estar basades en diversos criteris, com ara adreces IP d'origen i destí, ports de comunicació, protocols, etc.
- Polítiques de seguretat: Les polítiques determinen el comportament per defecte del tallafoc quan no s'aplica cap regla específica. Aquestes polítiques poden ser de denegació (block all) o de permís (allow all) per defecte.
- Accions de les regles: Les regles poden especificar diverses accions a realitzar amb els paquets que coincideixen amb les seves condicions, com ara acceptar-los, rebutjar-los, deixar-los passar sense alteració, registrar-los, etc.

Per configurar un tallafocs per comptabilitzar el trànsit que passa per una determinada regla, es pot afegir la clàusula counter a la regla específica. Aquesta clàusula permet que el tallafocs comptabilitzi el nombre de paquets o bytes que coincideixen amb aquesta regla i en registri els estadístics. Quan es fa una consulta sobre aquesta regla, es pot obtenir el nombre total de paquets o bytes que han estat acceptats o rebutjats. Això és útil per supervisar i avaluar el trànsit de xarxa i fer ajustaments a les polítiques de seguretat si cal.

La configuració de Tallafocs la farem amb nftables, és una eina per a la configuració de tallafocs en Linux, destinada a substituir eines més antigues com iptables. Ofereix una sintaxi més simple i una estructura modular per configurar taules, cadenes i regles que governen el tràfic de xarxa.

La comprovació s'anirà fent amb els diferents monitors i entre els diferents pings dins la xarxa o utilitzant el servei que li hem implementat la nova norma.

Les normes que hem pensat que s'han de implementar són:

- Filtrat d'Entrada (Input):
  Permetre trànsit des de les xarxes internes cap a serveis específics.
  Restringir l'accés no desitjat des de l'exterior excepte els serveis exposats com DNS i SSH en la DMZ.
- Filtrat de Sortida (Output):
  Monitoritzar i potencialment limitar el trànsit de sortida des dels servidors i routers per prevenir activitat maliciosa o no desitjada.
- Reenviament de Paquets (Forward):
  Permitir reenviament entre xarxes internes segons les polítiques de seguretat.
  Restringir el reenviament de la xarxa troncal a la DMZ i viceversa, excepte per als serveis permesos.
- NAT (Network Address Translation):
  Masquerar l'adreça de les xarxes internes quan accedeixen a Internet.
  Configurar redireccions específiques per permetre l'accés als serveis de la DMZ des de l'exterior.

Normes Específiques de Firewall

- Cadena INPUT
  Permetre el trànsit entrant al port SSH (22) des de qualsevol lloc per als monitors.

Permetre el trànsit entrant als serveis DNS i SSH en la DMZ des de l'exterior.
Permetre ICMP (ping) entre totes les xarxes per facilitar la monitorització i diagnòstic.

- Cadena FORWARD
  Permetre reenviament entre la xarxa DMZ i la xarxa de clients per a cert trànsit (p.ex., consultes DNS).
  Bloquejar tot el trànsit que no compleixi amb les polítiques específiques de connectivitat.
- Cadena OUTPUT
  Registrar tot el trànsit de sortida dels servidors per a anàlisi i monitorització.
  Cadena POSTROUTING per NAT
  Aplicar masquerade per a trànsit sortint des de la xarxa DMZ i clients cap a Internet a través de l'interfície eth-troncal

Les taules de NAT ja l'hem creat anteriorment, per configurar aquesta mateixa, així que implementarem les noves normes dins d'aquesta.

Podem mirar la taula actual fent: nft list ruleset
I utilitzarem el mode interactiu per anar creant les diferents normes, per entrar executar: nft -i

Anirem pas a pas executant les diferents comandes, amb el raonament de cada norma:

**** Tallafocs en Router d'accés**

La cadena prerouting s'utilitza generalment per a decisiones de NAT abans que les decisions de rutatge siguin preses.

```
add chain nat prerouting {type nat hook prerouting priority 0; policy accept; }
```

La cadena postrouting s'utilitza per a operacions de NAT després que les decisions de rutatge siguin preses, típicament per a masquerading o SNAT, ja la tenim creada per la configuració anterior de la NAT, però sinó es faria:

```
add chain ip nat postrouting {type nat hook postrouting priority 0; policy accept; }
```

La configuració per connectar a una xarxa a Internet compartint l'adreça IP del router de sortida, és com hem configurat per la NAT, per això tenim en la , sino s'hauria de fer:

```
add rule ip nat postrouting oifname "eth-troncal" masquerade
```

Aquesta regla permet a tots els dispositius de la xarxa local accedir a Internet amb l'adreça IP del router.

La cadena output es fa servir per a filtrar el tràfic que surt del host abans que aquest sigui enviat.

```
add chain ip nat output { type filter hook output priority 0; policy accept; }
```

Actualment la llista de nft tables és així:

```
table inet filter {
	chain input {
		type filter hook input priority filter; policy accept;
	}

	chain forward {
		type filter hook forward priority filter; policy accept;
	}

	chain output {
		type filter hook output priority filter; policy accept;
	}
}
table ip nat {
	chain postrouting {
		type nat hook postrouting priority srcnat; policy accept;
		oifname "eth-troncal" masquerade
	}

	chain prerouting {
		type nat hook prerouting priority filter; policy accept;
	}
```

```
        chain output {
                type nat hook output priority filter; policy accept;
        }
}
```

Però necessitem una configuració on es bloquegi tot menys les normes que tinguem implementades, així que haurem d'actualitzar les chains de input, forward i output:

Borrar les chains actuals:

```
delete chain inet filter input
delete chain inet filter forward
delete chain inet filter output
```

Actualitzar la política d'aquestes cadenes, i les comandes seran:

```
add chain inet filter input { type filter hook input priority 0; policy drop; }
add chain inet filter forward { type filter hook forward priority 0; policy drop; }
add chain inet filter output { type filter hook output priority 0; policy drop; }
```

La política per defecte per les cadenes és drop, el que significa que tot el tràfic que arribi i no coincideixi amb cap regla específica serà descartat. Això estableix una postura de seguretat "denegar per defecte".

La nova configuració que s'ha de guardar en el fitxer de /etc/nftables.conf
Per fer això, executar: nft list ruleset > /etc/nftables.conf
Guardar els canvis amb: systemctl restart nftables

Per la primera configuració aplicada a través dels monitors estaran al fitxer:

1-5-firewall-pingrouteracces.txt

Seguidament, volem tenir un log de totes les activitats, aixi que per cada activitat o servei o acció utilitzada, posarem la línia de guardar l'acció el el log específic del firewall.
Per això s'ha de descarregar el servei de: rsyslog
Executant: apt install rsyslog

Guardar en el seu fitxer de configuració que tots els missatges del kernel, que seran els que rebi el tallafocs, es guardin en un log, fitxer que guardarà tots els missatges importants que es puguin rebre.
Aquests es podran trobar a : /var/log/syslog
Però al tenir tants missatges del servidor, serà molt important utilitzar la eina de "grep" per anar filtrant segons els missatges que volguem consultar que s'hagin guardat.

Si volem que es guardi en un fitxer de logs especificament per les nftables es pot fer així:
Configurar la carpeta on es guardaran els logs: touch /var/log/nftables.log
Donar privilegis: chown 644 /var/log/nftables.log
chown root:root /var/log/nftables.log

I fer un fitxer de configuració per aquest log en el servei de rsyslog:
/etc/rsyslog.d/nftables.conf

```
:msg, contains,"nftables" /var/log/nftables.log
& stop
```

Reiniciar el servei: systemctl restart rsyslog
I podrem mirar els resultats en el fitxer: cat /var/log/nftables.log

O mirant.ho en directe fent: tail .-f /var/log/syslog

Per configurar correctament un tallafocs hem d'anar comprovant els seveis que hi té accés i com es poden implementar normes per protegir les xarxes internes, i verificar una vegada implementat que té un funcionament correcte:

SERVEI SSH:
Pels serveis utilitzarem la taula de nft de "filter", ja que serà la que deixarà o no les diferents connexions.

Permet l'accés SSH des de xarxes internes especifiques o adreces IP de confiança

```
add rule inet filter input ip saddr { 10.1.20.0/24, 10.1.10.0/28, 192.168.1.0/24 } tcp
dport 22 accept
```

Registrar qualsevol intent d'accés SSH per a auditories de seguretat

```
add rule inet filter input tcp dport 22 log prefix  "SSH attempt: " accept
```

Limitar la taxa d'intents d'accés per prevenir atacs de força bruta

```
add rule inet filter input tcp dport 22 limit rate 3/minute accept
```

La nova configuració que s'ha de guardar en el fitxer de /etc/nftables.conf
Per fer això, executar: nft list ruleset > /etc/nftables.conf
Guardar els canvis amb: systemctl restart nftables

Les verificacions estan al fitxer fetes des dels monitor : 1-5.firewall-valssh.txt
On es pot veure que es pot fer les ssh sense problema en el dmz i en els clients, però en la troncal no deixa entrar en les ssh.
Si entrem als logs i fem un filtratge segons el missatge que li hem posat: "SSH attempt: " podem veure les diferents entrades, com un ssh de entel a 10.1.10.1 o eth-troncal:

```
/var/log/syslog:2024-05-07T13:10:37.466206+02:00 routeracces kernel: [
302.374615]  SSH acces attempt:IN=eth-troncal OUT=
MAC=08:00:27:00:00:01:00:e0:4c:68:09:cd:08:00 SRC=192.168.1.24 DST=192.168.1.26
LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=13089 DF PROTO=TCP SPT=50909 DPT=22
WINDOW=64240 RES=0x00 SYN URGP=0
```

O un ssh del localhost utilitzant el port 22

/var/log/syslog:2024-05-07T13:32:25.068844+02:00 routeracces kernel: [1609.978670] SSH attempt:IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:86:dd SRC=0000:0000:0000:0000:0000:0000:0000:0001 DST=0000:0000:0000:0000:0000:0000:0000:0001 LEN=72 TC=16 HOPLIMIT=64 FLOWLBL=273674 PROTO=TCP SPT=35200 DPT=22 WINDOW=512 RES=0x00 ACK URGP=0

La configuració total del firewall del router d'accés esta el en fitxer:

1-5-firewall-routeracces.txt

**** Tallafocs en Router Acces**

```
# Regles per la cadena input
nft add rule inet filter input ip saddr 10.1.10.0/28 tcp dport 22 counter accept
nft add rule inet filter input ip saddr 10.1.20.0/24 tcp dport 22 counter accept
nft add rule inet filter input iifname "eth-troncal" ip protocol icmp counter accept
nft add rule inet filter input iifname "eth-dmz" ip protocol icmp counter accept
nft add rule inet filter input iifname "eth-troncal" counter accept
nft add rule inet filter input log prefix '"DROP INPUT: "' drop

# Crear la cadena forward
nft add chain inet filter forward { type filter hook forward priority 0; policy drop; }

# Reglas para la cadena forward
nft add rule inet filter forward iifname "eth-troncal" oifname "eth-dmz" ct state { established, related } counter accept
nft add rule inet filter forward iifname "eth-dmz" oifname "eth-troncal" tcp dport {80, 443, 53} counter accept
nft add rule inet filter forward ip saddr 10.1.10.0/28 oifname "eth-troncal" counter accept
nft add rule inet filter forward ip saddr 10.1.20.0/24 oifname "eth-troncal" counter accept
nft add rule inet filter forward ip saddr 10.1.10.0/28 ip daddr 10.1.20.0/24 counter accept
nft add rule inet filter forward ip saddr 10.1.20.0/24 ip daddr 10.1.10.0/28 counter accept


nft add rule inet filter forward log prefix '"DROP FORWARD: "' drop

# Crear la cadena output
nft add chain inet filter output { type filter hook output priority 0; policy drop; }

# Reglas para la cadena output
nft add rule inet filter output ip saddr 10.1.10.0/28 tcp dport 22 counter accept
```

nft add rule inet filter output ip saddr 10.1.20.0/24 tcp dport 22 counter accept
nft add rule inet filter output oifname "eth-troncal" counter accept
nft add rule inet filter output oifname "eth-troncal" ip protocol icmp counter accept
nft add rule inet filter output oifname "eth-dmz" ip protocol icmp counter accept
nft add rule inet filter output tcp sport 22 counter accept
nft add rule inet filter output log prefix '"DROP OUTPUT: "' drop

“nft add table inet filter: Crea una nova taula anomenada "filter" en l'espai de noms "inet".
nft add chain ... { type filter hook ... policy drop; }: Crea cadenes de filtratge "input", "forward" i "output" amb polítiques predeterminades per descartar paquets que no coincideixin amb cap regla.
nft add rule inet filter ... counter accept: Afegeix regles específiques per permetre el trànsit segons l'adreça IP, port, interfície, i protocol. L'acció accept permet el trànsit, mentre que counter permet comptar els paquets i bytes que coincideixen amb la regla.
nft add rule ... log prefix ... drop: Registra els paquets que seran descartats, útil per a depuració i seguiment d'intents d'accés no autoritzats o configuracions errònies.
Configuració de NAT (nft add table ip nat ...): Estableix regles de NAT per gestionar com els paquets surten de la xarxa, incloent el "masquerading" que és comú en entorns on múltiples màquines privades accedeixen a Internet a través d'una única adreça IP pública.

Posteriorment si volem que la configuració quedi, haurem d’executar nft -f /etc/nftables.conf per assegurar que compila correctament, a continuació nft list ruleset > /etc/nftables.conf. Ara per reiniciar i aplicar la configuració fem un systemctl restart nftables.

La configuració final del router accés serà:
/etc/nftables.conf

```
table inet filter {
	chain input {
		type filter hook input priority filter; policy drop;
		ip saddr 10.1.10.0/28 tcp dport 22 counter packets 0 bytes 0 accept
		ip saddr 10.1.20.0/24 tcp dport 22 counter packets 251 bytes 21248 accept
		iifname "eth-troncal" ip protocol icmp counter packets 4 bytes 336 accept
		iifname "eth-dmz" ip protocol icmp counter packets 0 bytes 0 accept
		iifname "eth-troncal" counter packets 19 bytes 1215 accept
		log prefix "DROP INPUT: " drop
	}
```

```
        chain forward {
                type filter hook forward priority filter; policy drop;
                iifname "eth-troncal" oifname "eth-dmz" ct state { established, related }
counter packets 0 bytes 0 accept
                iifname "eth-dmz" oifname "eth-troncal" tcp dport 80 counter packets 0
bytes 0 accept
                iifname "eth-dmz" oifname "eth-troncal" tcp dport 443 counter packets
0 bytes 0 accept
                iifname "eth-dmz" oifname "eth-troncal" tcp dport 53 counter packets 0
bytes 0 accept
                ip saddr 10.1.10.0/28 oifname "eth-troncal" counter packets 0 bytes 0
accept
                ip saddr 10.1.20.0/24 oifname "eth-troncal" counter packets 0 bytes 0
accept
                ip saddr 10.1.10.0/28 ip daddr 10.1.20.0/24 counter accept
                ip saddr 10.1.20.0/24 ip daddr 10.1.10.0/28 counter accept
                log prefix "DROP FORWARD: " drop
        }

        chain output {
                type filter hook output priority filter; policy drop;
                ip saddr 10.1.10.0/28 tcp dport 22 counter packets 0 bytes 0 accept
                ip saddr 10.1.20.0/24 tcp dport 22 counter packets 0 bytes 0 accept
                oifname "eth-troncal" counter packets 1 bytes 56 accept
                oifname "eth-troncal" ip protocol icmp counter packets 4 bytes 336
accept
                oifname "eth-dmz" ip protocol icmp counter packets 0 bytes 0 accept
                tcp sport 22 counter packets 152 bytes 18296 accept
                log prefix "DROP OUTPUT: " drop
        }
}
table ip nat {
        chain OUTPUT {
                type nat hook output priority filter; policy accept;
        }

        chain PREROUTING {
                type nat hook prerouting priority filter; policy accept;
        }

        chain POSTROUTING {
                type nat hook postrouting priority srcnat; policy accept;
                oifname "eth-troncal" masquerade
        }
```

}

**** Tallafocs en Router intern**

Pel tallafoc del router intern, s`ha de configurar com el tallafocs del router d'accés, simplement amb menys normes, ja que no necessitem pensar en l'accés a internet, que aquest ja se'n ocupa el router d'accés.

Cadena input: Aquesta cadena gestiona els paquets que són destinats a la màquina on s'executa el firewall. Les regles d'aquesta cadena determinen com es tracten aquests paquets. En la teva configuració, la política per defecte (policy drop) descarta tots els paquets que no compleixen amb les regles específiques que has definit.

Cadena output: Aquesta cadena gestiona els paquets que s'originen a la màquina on s'executa el firewall. Les regles d'aquesta cadena determinen com es tracten aquests paquets. En la teva configuració, la política per defecte també és drop, de manera que tots els paquets que no compleixen amb les regles específiques són descartats.

Cadena forward: Aquesta cadena gestiona els paquets que simplement passen per la màquina on s'executa el firewall (és a dir, els paquets que no s'originen ni es destinen a aquesta màquina). Les regles d'aquesta cadena determinen com es tracten aquests paquets. De nou, la política per defecte és drop.
Per afegir regles a aquestes cadenes utilitzant nft, pots utilitzar la següent sintaxi:

Ja tenim les chains de input, forward i output de filter, així que no caldrà crear-ne cap més:

```
cat /etc/nftables.conf
        #!/usr/sbin/nft -f

        flush ruleset

        table inet filter {
                chain input {
                        type filter hook input priority filter;
                }
                chain forward {
                        type filter hook forward priority filter;
                }
                chain output {
                        type filter hook output priority filter;
                }
```

}

Amb aquesta configuració inicial, primer haurem de posar que les cadenes de filtratge tinguin policy drop, és a dir, que haurem de borrar el contingut de nfttables.conf i des del mode interactiu de : nft -i

Borrar les chains actuals:

delete chain inet filter input
delete chain inet filter forward
delete chain inet filter output

Actualitzar la política d'aquestes cadenes, i les comandes seran:

add chain inet filter input { type filter hook input priority 0; policy drop; }
add chain inet filter forward { type filter hook forward priority 0; policy drop; }
add chain inet filter output { type filter hook output priority 0; policy drop; }

La política per defecte per les cadenes és drop, el que significa que tot el tràfic que arribi i no coincideixi amb cap regla específica serà descartat. Això estableix una postura de seguretat "denegar per defecte".

La nova configuració que s'ha de guardar en el fitxer de /etc/nftables.conf
Per fer això, executar: nft list ruleset > /etc/nftables.conf
Guardar els canvis amb: systemctl restart nftables

Ara si fem un ping no deixarà fer en el router intern, així que haurem de configurar per les diferents cadenes, la configuració de connexió en la xarxa:

*** Configuració per la cadena input:**

Aquesta regla permet el trànsit que prové de la interfície de loopback (interfície lo), la qual s'utilitza per a la comunicació interna del propi dispositiu.

add rule inet filter input iifname "lo" accept

Aquesta regla permet el trànsit associat amb connexions ja establertes o relacionades.

add rule inet filter input ct state established,related accept

Aquesta regla permet els paquets ICMP tipus "echo-request" amb una limitació de velocitat de 3 paquets per segon i un contador màxim de 18 paquets i 1512 bytes. Aquesta regla pot ajudar a controlar i limitar la quantitat de trànsit ICMP "echo-request" que entra al dispositiu.

add rule inet filter input icmp type echo-request limit rate 3/second counter packets 18 bytes 1512 accept

Aquesta regla permet el trànsit TCP amb una adreça d'origen de 10.1.10.11, 10.1.20.11 o 192.168.1.28 i un port de destinació de 22 (el port SSH). Aquesta regla està destinada a permetre la connexió SSH des d'aquests monitors.

```
add rule inet filter input ip saddr { 10.1.10.11, 10.1.20.11, 192.168.1.28 } tcp dport 22 counter packets 0 bytes 0 accept
```

Aquestes comandes afegirien les dues regles per permetre les peticions de ping (paquets ICMP tipus echo-request) que provenen de les subxarxes 10.1.10.0/28 i 10.1.20.0/24 a la cadena input del teu tallafoc.

```
add rule inet filter input ip saddr 10.1.10.0/28 icmp type echo-request accept
add rule inet filter input ip saddr 10.1.20.0/24 icmp type echo-request accept
```

.

Tenint la cadena de input :

```
chain input {
        type filter hook input priority filter; policy drop;
        iifname "lo" accept
        ct state established,related accept
        icmp type echo-request limit rate 3/second counter packets 18 bytes 1512 accept
        ip saddr { 10.1.10.11, 10.1.20.11, 192.168.1.28 } tcp dport 22 counter packets 0 bytes 0 accept
        ip saddr 10.1.10.0/28 icmp type echo-request accept
        ip saddr 10.1.20.0/24 icmp type echo-request accept
}
```

*** Configuració per la cadena output:**

Aquesta regla permet els paquets ICMP tipus "echo-request" que surten del dispositiu amb una adreça d'origen a la subxarxa 10.1.20.0/24.

```
add rule inet filter output ip saddr 10.1.20.0/24 icmp type echo-request accept
```

Aquesta regla permet els paquets ICMP tipus "echo-request" que surten del dispositiu amb una adreça d'origen a la subxarxa 10.1.10.0/28.

```
add rule inet filter output ip saddr 10.1.10.0/28 icmp type echo-request accept
```

Aquesta regla permet els paquets ICMP tipus "echo-request" que tenen com a destinació la subxarxa 10.1.20.0/24.

```
add rule inet filter output ip daddr 10.1.20.0/24 icmp type echo-request accept
```

Aquesta regla permet els paquets ICMP tipus "echo-request" que tenen com a destinació la subxarxa 10.1.10.0/28.

add rule inet filter output ip daddr 10.1.10.0/28 icmp type echo-request accept

Aquesta regla permet els paquets ICMP tipus "echo-reply" que tenen com a destinació la subxarxa 10.1.10.0/28.

add rule inet filter output ip daddr 10.1.10.0/28 icmp type echo-reply accept

Aquesta regla permet els paquets ICMP tipus "echo-reply" que tenen com a destinació la subxarxa 10.1.20.0/24.

add rule inet filter output ip daddr 10.1.20.0/24 icmp type echo-reply accept

Per afegir la regla que permet el trànsit SSH sortint a la teva cadena output, pots utilitzar la següent comanda:

nft add rule inet filter output tcp sport 22 accept

Tenint la cadena de output:

```
chain output {
        type filter hook output priority filter; policy drop;
        ip saddr 10.1.20.0/24 icmp type echo-request accept
        ip saddr 10.1.10.0/28 icmp type echo-request accept
        ip daddr 10.1.20.0/24 icmp type echo-request accept
        ip daddr 10.1.10.0/28 icmp type echo-request accept
        ip daddr 10.1.10.0/28 icmp type echo-reply accept
        ip daddr 10.1.20.0/24 icmp type echo-reply accept
        tcp sport 22 accept
}
```

*** Configuració per la cadena forward:**

Aquesta regla permet el trànsit que està associat amb connexions ja establertes o relacionades.

add rule inet filter forward ct state established,related accept

Aquesta regla permet el trànsit que entra a través de la interfície "eth-clients".

add rule inet filter forward iifname "eth-clients" accept

Aquesta regla permet el trànsit que entra a través de la interfície "eth-dmz".

add rule inet filter forward iifname "eth-dmz" accept

Aquesta regla permet el trànsit que entra a través de la interfície "eth-dmz" i surt a través de la interfície "eth-clients".

add rule inet filter forward iifname "eth-dmz" oifname "eth-clients" accept

Aquesta regla permet els paquets ICMP tipus "echo-request" que tenen com a origen la subxarxa 10.1.10.0/28 i com a destinació la subxarxa 10.1.20.0/24.

add rule inet filter forward ip saddr 10.1.10.0/28 ip daddr 10.1.20.0/24 icmp type echo-request accept

Aquesta regla permet els paquets ICMP tipus "echo-request" que tenen com a origen la subxarxa 10.1.20.0/24 i com a destinació la subxarxa 10.1.10.0/28.

add rule inet filter forward ip saddr 10.1.20.0/24 ip daddr 10.1.10.0/28 icmp type echo-request accept

Tenint la cadena de forward:

```
chain forward {
        type filter hook forward priority filter; policy drop;
        ct state established,related accept
        iifname "eth-clients" accept
        iifname "eth-dmz" accept
        iifname "eth-dmz" oifname "eth-clients" accept
        ip saddr 10.1.10.0/28 ip daddr 10.1.20.0/24 icmp type echo-request accept
        ip saddr 10.1.20.0/24 ip daddr 10.1.10.0/28 icmp type echo-request accept
}
```

La nova configuració que s'ha de guardar en el fitxer de /etc/nftables.conf
Per fer això, executar: nft list ruleset > /etc/nftables.conf
Guardar els canvis amb: systemctl restart nftables

Les evidencies dels pings entre els monitors, estan en el fitxer :

1-5-firewall-pingrouterintern.txt

***** Serveis del router intern:**

* **SSH pels monitors:**

Aquesta comanda permet les connexions SSH des dels monitors amb les adreces IP especificades cap al port 22 del dispositiu:

add rule inet filter input ip saddr { 10.1.10.11, 10.1.20.11, 192.168.1.28 } tcp dport 22 accept

Es permeten les respostes sortints a les connexions SSH:

add rule inet filter output tcp sport 22 accept

*** Protocol DHCP:**

(per pròximes conexions amb la xarxa clients,que utilitzà futurament quan fem una implementació de dhcp en els possibles clients)

Aquesta comanda permet el trànsit DHCP que entra a través de la interfície "eth-clients" amb els ports UDP 67 i 68:

```
add rule inet filter input iifname “eth-clients”  udp dport {67,68} counter accept
```

*** Protocol DNS:**

(Per pròximes implementacions del servei que farem futurament)

Aquestes comandes permeten el trànsit DNS que entra amb els ports TCP i UDP 53:

```
add rule inet filter input tcp dport 53 accept
add rule inet filter input udp dport 53 accept
```

*** Protocol Nagios (SNMP):**

(Per pròximes implementacions del servei que farem futurament)

Aquestes comandes permeten el trànsit SNMP (port 161) i el trànsit Nagios (port 5666) que entra amb els ports UDP i TCP:

```
add rule inet filter input udp dport 161 accept
add rule inet filter input tcp dport 161 accept

add rule inet filter input udp dport 5666 accept
add rule inet filter input tcp dport 5666 accept
```

La nova configuració que s’ha de guardar en el fitxer de /etc/nftables.conf
Per fer això, executar: nft list ruleset > /etc/nftables.conf
Guardar els canvis amb: systemctl restart nftables

Les evidències dels ssh entre els monitors, estan en el fitxer :

```
1-5-firewall-sshrouterintern.txt
```

Deixa fer ssh entre els monitors, però des de la xarxa troncal i des de una màquina exterior, no poden establir connexió.

Les evidències de naggios i dns i dhcp entre els monitors, estan en el fitxer:

```
1-5-firewall-serveisrouterintern.txt
```

La configuració final del router intern seria:
cat /etc/nftables.conf

```
table inet filter {
        chain input {
                type filter hook input priority filter; policy drop;
```

```
                iifname "lo" accept
                ct state established,related accept
                icmp type echo-request limit rate 3/second counter packets 26 bytes
2184 accept
                ip saddr { 10.1.10.11, 10.1.20.11, 192.168.1.28 } tcp dport 22 counter
packets 3 bytes 180 accept
                ip saddr 10.1.10.0/28 icmp type echo-request accept
                ip saddr 10.1.20.0/24 icmp type echo-request accept
                ip saddr { 10.1.10.11, 10.1.20.11, 192.168.1.28 } tcp dport 22 accept
                tcp dport 53 accept
                udp dport 53 accept
                udp dport 161 accept
                udp dport 5666 accept
                tcp dport 161 accept
                tcp dport 5666 accept
                iifname "eth-clients" udp dport { 67, 68 } counter packets 0 bytes 0
accept
        }

        chain output {
                type filter hook output priority filter; policy drop;
                ip saddr 10.1.20.0/24 icmp type echo-request accept
                ip saddr 10.1.10.0/28 icmp type echo-request accept
                ip daddr 10.1.20.0/24 icmp type echo-request accept
                ip daddr 10.1.10.0/28 icmp type echo-request accept
                ip daddr 10.1.10.0/28 icmp type echo-reply accept
                ip daddr 10.1.20.0/24 icmp type echo-reply accept
                tcp sport 22 accept
        }

        chain forward {
                type filter hook forward priority filter; policy drop;
                ct state established,related accept
                iifname "eth-clients" accept
                iifname "eth-dmz" accept
                iifname "eth-dmz" oifname "eth-clients" accept
                ip saddr 10.1.10.0/28 ip daddr 10.1.20.0/24 icmp type echo-request
accept
                ip saddr 10.1.20.0/24 ip daddr 10.1.10.0/28 icmp type echo-request
accept
        }
}
```

La configuració total del firewall del router intern esta el en fitxer:

1-5-firewall-routerintern.txt

Les proves finals fetes entre els monitors de la xarxa i amb els dos firewalls activats un en cada cada router, es poden veure en el fitxer:

1-5-firewall-evidenciesfinals.txt

Fitxers involucrats:
- /etc/nftables.conf
Per la configuració del tallafocs
- nft -i
Mode interactiu per implementar totes les regles del firewall.

Fitxers d'evidència:
Router d'accés: 1-5-firewall-routeracces.txt
Router intern: 1-5-firewall-routerintern.txt

Verificacions:

Verificació router d'accés:
1-5-firewall-pingrouteracces.txt
1-5-firewall-sshrouteracces.txt

Verificació router intern:
1-5-firewall-pingrouterintern.txt
1-5-firewall-sshrouterintern.txt
1-5-firewall-serveisrouterintern.txt

Verificació final:
1-5-firewall-evidenciesfinals.txt
Son les proves dels monitors que s'han fet amb els dos firewalls activats en cada router.

Es poden veure els resultats de l'execució de les explicacions anteriors

Fonts d'informació:

Manual de Virtual Networking de vb: https://www.virtualbox.org/manual/ch06.html
dhcp server en vb: https://www.virtualbox.org/manual/ch08.html#vboxmanage-dhcpserver
documentació de routers en vb:
https://forums.virtualbox.org/viewtopic.php?f=35&t=96608#p468780
Tipus de xarxes en vb:
https://www.redeszone.net/tutoriales/redes-cable/configuracion-red-maquina-virtual-virtualbox/#519933-opciones-de-red-disponibles-en-una-maquina-virtual
Configuració network general: https://wiki.debian.org/NetworkConfiguration
Taules nft debian : https://wiki.debian.org/nftables
Nat tables wiki:
https://wiki.nftables.org/wiki-nftables/index.php/Performing_Network_Address_Translation_(NAT)
configuracio resolv.conf: https://wiki.debian.org/resolv.conf
ssh debian: https://wiki.debian.org/SSH
ssh servidor debian: https://servidordebian.org/es/buster/config/remote_access/ssh_server
firewall utilitzant nftables:
https://www.redeszone.net/tutoriales/seguridad/nftables-firewall-linux-configuracion/
fiewall nftwables archilinux: https://wiki.archlinux.org/title/nftables
inici nftables red hat:
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/getting-started-with-nftables_configuring-and-managing-networking
Exemples nftables: https://wiki.gentoo.org/wiki/Nftables/Examples