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?

routeracces

eth-troncal -> IP: (asignada per dhcp) - MAC: 08:00:27:00:00:01 - adaptador pont

· eth-dmz -> IP: 10.1.10.1 - MAC: 08:00:27:01:10:01 - redInterna(dmz)

routerinter

· eth-dmz -> IP: 10.1.10.2 - MAC: 08:00:27:01:10:02-redInterna(dmz)

· clients -> IP: 10.1.20.1 - MAC: 08:00:27:01:20:01 - redInterna(clients)

monitordmz  
 eth0 -> IP: 10.1.10.11 - MAC: 08:00:27:01:00:11- redInterna(dmz)

monitorclients  
 eth0 -> IP: 10.1.20.11 - MAC: 08:00:27:01:00:12- redInterna(clients)

- Com es configuren els noms de les interfícies a les màquines de l'escenari?

Per configurar el nom i que es quedi sempre hem de crear un fitxer en nano /etc/udev/rules.d/10-network.rules i añadim la següent linea  
SUBSYSTEM=="net", ACTION=="add", ATTR{address}=="MAC de LA MAQUINA", NAME="nom\_interfaz"

i després anem al fitxer etc/network/interfaces i configurem les ip’s de manera estatica

- Com es configura un router per a que actuï com a tal? Com s'afegeixen rutes estàtiques a un equip?

Per configurar el router fem el següent:

sudo nano /etc/sysctl.conf  
net.ipv4.ip\_forward = 1  
descomentas esta linea i reinicias el servicio  
sudo sysctl -p(per reiniciar el servei)

Per afegir rutes estàtiques i que es guardin per sempre hem de fer:  
up ip route add {ip/mask destí} via {quin router va} dev{per quina interfaç surt}

per exemple en el router d’acces hem fet

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

- Quina és la taula d'encaminament de cadascun dels routers del escenari? Hi ha com a mínim una ruta per a cada xarxa?  
fent ip route show

Router intern  
default via 10.1.10.1 dev eth-dmz onlink

10.1.10.0/28 dev eth-dmz proto kernel scope link src 10.1.10.2

10.1.20.0/24 dev clients proto kernel scope link src 10.1.20.1

169.254.0.0/16 dev eth-dmz scope link metric 1000

Router acces

default via 192.168.1.1 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

169.254.0.0/16 dev eth-troncal scope link metric 1000

192.168.1.0/24 dev eth-troncal proto kernel scope link src 192.168.1.136   
  
Podem veure que si hi ha una ruta mínim per cada xarxa.

- Quin és el router per defecte de cada xarxa? Quin és el router per defecte de cada router?

XARXA TRONCAL: router d’access

XARXA DMZ: router intern

XARXA CLIENTS:router intern

ROUTER INTERN: router access

ROUTER ACCES: router de casa, amb el que accedim a internet.

- 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.

connectats si és el cas) tenen les màquines virtuals de l'escenari?

routeracces

eth-troncal -> per DHCP, es necesari que sigui per DHCP perque la ip ha de estar en el rang de la IP del router que té conexió a internet, que aquest pot cambiar.

· eth-dmz -> estatica

routerinter

· eth-dmz ->Estatica

· clients -> Estatica

monitordmz  
 eth0 -> Estatica

monitorclients  
 eth0 -> Estatica  
  
Les altres son estaticas perque ens va bé que sempre siguin las mateixes, per posar-les en el rang de la seva xarxa i que sempre sigui la mateixa

- Quines comunicacions es permeten entre cadascuna de les xarxes (Internet, DMZ, clients)?

Sense configurar el NAT podem fer ping a totes les reds però la unica maquina que te accès a internet es el router d’acces.

Evidencia pingsRouteracces:  
ping al Router Intern a (10.1.20.1, 10.1.10.2)

Al monitor DMZ(10.1.10.11)

Al monitor Client(10.1.20.11)

Evidencia pingsRouterIntern:

ping al router extern a (10.1.10.1,192.168.1.136)

Al monitor DMZ(10.1.10.11)

Al monitor Client(10.1.20.11)

També podem veure que els dos monitors tenen accés a tot.

CONFIGURACIÓ DE LA NAT

Tenint aquesta configuració en el router acces(/etc/nftables.conf)

chain postrouting {

type nat hook postrouting priority srcnat;

ip saddr 10.1.10.0/28 masquerade;

ip saddr 10.1.20.0/24 masquerade;

}

No podem fer ping a google ja que no tenim configurat el DNS pero desde qualsevol equip podem fer ping al 8.8.8.8.

Veure en evidencias

pingRouterIntern-8.8.8.8

pingRouterAcces-8.8.8.8

pingMonitorDMZ-8.8.8.8

pingMonitorClients-8.8.8.8

També hem fet que el monitor client pugui conectar-se al root per ssh amb claus privades/públicas

- De manera particular, quines accions s'han fet per a maximitzar la seguretat?  
El primer pas de securització extra que hem optat per fer, es generar distintes keys per cada conexió al root de ssh, de forma que s’ailli la “vulnerabilitat” de perdre una clau o que es filtri d’alguna forma, d’altra banda i per evitar atacs de força bruta, hem aplicat fail2ban en el monitor de la xarxa dmz, sobre el servei ssh, de forma que en intentar conectarse 3 vegades, i fallar la contrasenya, es rep un ban de 5 minuts, dificultat per complet aquest modus operandi, l’instalació del fail2ban l’hem fet a partir de:

apt install fail2ban, i seguint les configuracions de la wiki proporcionada a clase, afegint els camps

[sshd]

maxrety = 3

al /fail2ban/config/jail.local i per arrelgar el bug esmentat DEFAULT]:

logtarget = SYSTEMD-JOURNAL

backend = systemd

enabled=true

bantime = 5m

ara per evitar que perdem la configuració al botar la maquina executarem les següents comandes: update-rc.d fail2ban defaults

systemctl restart fail2banservice

service fail2ban start

d’aquesta manera quedaria configurat el fail2ban.

- Com es configuren els tallafocs per filtrar paquets d'acord amb les comunicacions que es permeten?

En la xarxa de clients s’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, també els DNS i el NAGIOS poden fer consultes a DNS externes,

també s’ha de poder fer pings entre tota la estructura

també desde fora s’ha de poder fer ssh al servidor dmz

Per fer això posem en el forward del filter del router d'accés

chain forward{

type filter hook forward priority filter; policy drop;

ct state related,established accept  
 udp dport 53 ip saddr 10.1.10.3 accept

udp dport 53 ip saddr 10.1.10.4 accept

udp dport 53 ip saddr 10.1.10.5 accept

ip protocol icmp accept

ip daddr 10.1.10.11 tcp dport 22 accept

}

El router d’acces tanbé ha de permitir que li arribi trafic icmp desde qualsevol lloc

que nomes li arribi una conexió ssh desde els monitors de clients o la DMZ

chain input {

type filter hook input priority filter; policy drop;

ip protocol icmp accept

ip saddr 10.1.20.11 tcp dport 22 accept

ip saddr 10.1.10.11 tcp dport 22 accept

}

- Com es configura el tallafocs per a registri una determinada activitat?

tcp dport 22 log prefix "SSH Connection: " accept  
això fa que es guardin els intents de ssh

- Com es configura el tallafocs per a que comptabilitzi el trànsit que passa per una determinada regla?

tcp dport 22 counter log prefix "SSH Traffic: " accept

això contarà el transit que pasi per el port 22

- Com es configura el tallafocs per a balancejar càrrega entre dos servidors?

Per que els servidor DNS1 i DNS2 tinguin un balanceig de carga, fem en el router de acces

nft add rule nat prerouting dnat to numgen inc mod 2 map { \

0 : 10.1.10.1.3, \

1 : 10.1.10.1.4}

- Com es configura el tallafocs per a redirigir un port?

En el table inet nat posem

chain prerouting{

tcp dport 22 redirect to :1234

}

Això fa que tot del port 22 es redirigeixi per el port 1234.

També canviem en la configuracio del ssh que acepti per el port 1234

- Com es configura el tallafocs per a connectar una xarxa a Internet compartint l'adreça IP del router de sortida?

En el router d’acces fem

table inet nat {

chain postrouting {

type nat hook postrouting priority srcnat;

ip saddr 10.1.10.0/28 masquerade;

ip saddr 10.1.20.0/24 masquerade;

}

}

- Com es pot comprovar que la configuració anterior es correcta?

Hem vist que podem fer ping entre tots els equips

Els clients no poden fer ping al exterior ja que necesitan tenir una conexio previa per poder fer

Els monitors poden fer ssh als routers i entre ells.

- Com es guarda la configuració de nftables en un fitxer de manera que es carregui automàticament?   
systemctl enable nftables, fem que estigui obert el servei de nftables i cada cop que s’inicia la maquina executa el fitxer /etc/nftables.conf