Firewalling NOS: VyOS

1.-PREVI-I) Modifica la màquina VirtualBox "VyOS1" que vas utilitzar als anteriors exercicis de "routing" per a què ara tingui dues tarjes de xarxa, una en mode "adaptador pont" (la *eth0*) i una altra en mode "xarxa interna" (la *eth1*). A més, modifica la màquina VirtualBox "Ubuntu1" que també vas utilitzar anteriorment per a què tingui igualment una tarja de xarxa en mode "xarxa interna" (en la mateixa xarxa que "VyOS1"). Arrenca tot seguit ambdues màquines.

PREVI-II) Configura la màquina "VyOS1" de la següent manera:

* La seva tarja *eth0* haurà d'obtenir la configuració de xarxa (adreça IP, màscara, porta d'enllaç i servidors DNS) via DHCP. Els servidors DNS obtinguts hauran de ser, a més, els que el propi sistema VyOS utilitzi a nivell global

* La seva tarja *eth1* haurà de tenir una adreça IP i màscara fixa (concretament, la 10.1.1.1/8)

* Haurà d'implementar la capacitat de "DNS forwarding", a través de la tarja *eth1*, per tots els eventuals clients que pertanyin a la mateixa xarxa que ella (és a dir, a la xarxa 10.0.0.0/8). Els servidors DNS on es reenviaran les peticions seran els configurats globalment al propi sistema VyOS

* Haurà d'implementar un servidor DHCP per tota la xarxa 10.0.0.0/8. Concretament, haurà de repartir adreces IP entre 10.2.2.2 i 10.2.2.100, assignant com a porta d'enllaç dels possibles clients la IP 10.1.1.1 (és a dir, la IP de *eth1* del sistema VyOS) i assignant com a servidor DNS també la mateixa IP 10.1.1.1 (que és just on estarà funcionant el "DNS forwarder" indicat al paràgraf anterior)

NOTA: Per si no ho recordes, el que es demana en el paràgraf anterior es pot aconseguir de la següent manera:

```
configure
set interfaces ethernet eth0 address dhcp
set system name-server eth0
commit
set interfaces ethernet eth1 address 10.1.1.1/8
commit
edit service dns forwarding
set listen-address 10.1.1.1
set allow-from 10.0.0.0/8
set system
commit
exit
edit service dhcp-server shared-network-name unPool subnet 10.0.0.0/8
set subnet-id 1
set range unRang start 10.2.2.2
set range unRang stop 10.2.2.100
set option default-router 10.1.1.1
set option name-server 10.1.1.1
commit
exit
save
```

PREVI-III) Demana via DHCP la configuració de xarxa de la tarja *enp0s3* de "Ubuntu1" (ho pots fer per exemple executant *sudo dhclient -v enp0s3* o bé, si tens el servei NetworkManager en marxa, executant *nmcli con down nomconnexio && nmcli con up nomconnexio*).

* Comprova tot seguit que, efectivament, has obtingut una IP del rang pertinent (amb *ip -c a*), la porta d'enllaç pertinent (amb *ip -c r*) i el servidor DNS pertinent (amb *resolvectl dns*).

* Comprova, finalment, que les consultes DNS són correctament reenviades gràcies al "forwarder DNS" que hem implementat al sistema VyOS (ho pots comprovar executant per exemple *dig www.hola.com* i observant com obtens la resposta adient) però que qualsevol altre tràfic (com pot ser el de tipus ICMP -via *ping*- o una consulta HTTP -via *curl*-, etc, etc, etc) no funciona. La raó és simple: no s'ha habilitat el NAT per poder accedir a la xarxa d'IPs públiques que és Internet; és el que farem als propers apartats

NOTA: Teniu la informació de com configurar NAT a VyOS a https://docs.vyos.io/en/latest/configuration/nat/nat44.html

a) Executa les següents comandes al sistema VyOS:

configure
set nat source rule 1 outbound-interface name eth0
set nat source rule 1 source address 10.0.0.0/8
set nat source rule 1 translation address masquerade
commit
save

NOTA: Com totes les regles del tallafocs, les regles NAT **s´apliquen en ordre** segons el seu número de regla. En aquest cas concret, totes les línies anteriors pertanyen al mateix número de regla (la nº1) perquè de fet, formen una sola conceptualment (és a dir, es podria fer *edit nat source rule 100*) i, per tant, aquest detall ara mateix no és rellevant, però cal tenir-ho present per propers exercicis quan tinguem més d'una regla definida. En tot cas, és molt important recordar que a totes les regles del tallafocs, siguin NAT o de tipus "filter", en quant el paquet de xarxa inspeccionat concordi amb una regla determinada, s'hi aplicarà aquesta i es deixarà de llegir les regles que quedin encara posteriorment; si el paquet no concorda amb cap de les regles indicades, en el cas de les regles de tipus "filter" llavors s'hi aplicarà la regla establerta per defecte (*drop* o *accept*)

* ¿Per a què serveixen cadascuna de les comandes anteriors? ¿Ara ja es pot fer "ping" des de la màquina "Ubuntu1" a qualsevol IP o nom DNS d'Internet i es pot accedir via curl a qualsevol servidor web d'Internet?

* ¿Què mostra, al sistema VyOS, la comanda *show nat* (executada al mode de configuració)? ¿I la comanda *show nat source rules* (executada al mode operacional)? ¿I s*how nat source translations* (també del mode operacional)? ¿ I *show nat source statistics* (també del mode operacional)?

aII) Executa la següent comanda al sistema Ubuntu: *nc -l -p 4444* i tot seguit executa les següents comandes a la màquina VyOS:

configure
set nat destination rule 1 inbound-interface name eth0
set nat destination rule 1 protocol tcp
set nat destination rule 1 destination port 4444
set nat destination rule 1 translation address 10.2.2.2 <--Suposem que aquesta és la IP del sistema Ubuntu!
set nat destination rule 1 translation port 4444
commit
save

NOTA: La regla anterior té el mateix número que l'emprada a l'apartat previ perquè les regles SNAT i les regles DNAT es compten de forma independent

* ¿Per a què serveixen cadascuna de les comandes anteriors? ¿Què passa si, des de la teva màquina real, executes la comanda *nc iptarja.modeadap.tadorpont.maqVyOS 4444* ?

* ¿Què mostra, al sistema VyOS, la comanda *show nat* (executada al mode de configuració)? ¿I la comanda *show nat destination rules* (executada al mode operacional)? ¿I s*how nat destination translations* (també del mode operacional)? ¿ I *show nat destination statistics* (també del mode operacional)?

NOTA: Teniu la informació de com configurar el tallafocs a VyOS a https://docs.vyos.io/en/latest/configuration/firewall , i més en concret, a https://docs.vyos.io/en/latest/configuration/firewall/ipv4.html i també https://docs.vyos.io/en/latest/configuration/firewall/zone.html , així com també https://docs.vyos.io/en/latest/configuration/firewall/global-options.html i https://docs.vyos.io/en/latest/configuration/firewall/groups.html . En el cas particular d'implementar un "bridge" en un sistema VyOS, les regles a aplicar estan descrites a https://docs.vyos.io/en/latest/configuration/firewall/bridge.html

b) Executa les següents comandes al sistema VyOS:

configure
set firewall ipv4 input filter default-action drop
set firewall ipv4 forward filter default-action drop

set firewall ipv4 output filter default-action drop
commit

* ¿Què fan cadascuna de les línies anteriors? ¿Segueixen funcionant les consultes DNS fetes des de la màquina Ubuntu (per exemple amb *dig*)? ¿I les peticions HTTP (per exemple amb *curl*)? D'altra banda, ¿funcionen els "pings" fets des de la màquina real a la tarja *eth0* de la màquina VyOS? ¿Per què? ¿Què mostra al sistema VyOS la comanda del mode operational *show firewall [ipv4 | summary | statistics]* ?

bII) Executa les següents comandes al sistema VyOS:

configure
edit firewall ipv4 input filter rule 1
set source address 10.0.0.0/8
set destination address 10.1.1.1
set destination port 53,67,68,123 <--Els ports 67 i 68 són pel DHCP i el 123 pel NTP, que també cal obrir
set protocol udp
set action accept
commit
exit
edit firewall ipv4 output filter rule 1
####set destination port 53,67,68,123 <--No cal
set protocol udp
set action accept
commit
exit
edit firewall ipv4 input filter rule 2
set inbound-interface name eth0
set source port 53,67,68,123
set protocol udp
set action accept
commit
exit

NOTA: Tingues en compte que un "forwarder DNS" rep la petició dels clients ell mateix (és a dir, a través de la cadena "input") i llavors genera ell mateix una consulta DNS al servidor DNS principal (és a dir, sortint per la cadena "output"); no fa, per tant, cap reenviament i per això no utilitzem la cadena "forward".
NOTA: Recorda que el protocol UDP (així com l'ICMP) no incorporen el concepte de "connexió", així que el "truc" d'indicar l'estat "established" o "related" no funciona aquí. És per això que per poder rebre les respostes associades a les peticions vinculades a la regla "output" nº1 cal indicar la regla "input" nº2 explícitament
NOTA: Existeix la paraula especial "tcp_udp" per indicar que els ports indicats a les regles poden ser o bé TCP o bé UDP

* ¿Què fan cadascuna de les línies anteriors? ¿Funcionen ara les consultes DNS fetes des de la màquina Ubuntu (per exemple amb *dig*)? ¿Per què? ¿Què mostra al sistema VyOS la comanda del mode de configuració *show firewall*?

bIII) Executa les següents comandes al sistema VyOS:

configure
edit firewall ipv4 forward filter rule 1
set inbound-interface name eth1
set outbound-interface name eth0
set destination port 80,443
set protocol tcp
set action accept
commit
exit
edit firewall ipv4 forward filter rule 2
set inbound-interface name eth0
set outbound-interface name eth1
set state establised
set state related
set protocol tcp

set action accept
commit
exit

* ¿Què fan cadascuna de les línies anteriors? ¿Funcionen ara les peticions HTTP fetes des de la màquina Ubuntu (per exemple amb *curl*)?

bIV) Executa les següents comandes al sistema VyOS:

configure
edit firewall ipv4 forward filter rule 3
set inbound-interface name eth1
set outbound-interface name eth0
set icmp type 8
set icmp type 0
set action accept
commit
exit
edit firewall ipv4 forward filter rule 4
set inbound-interface name eth0
set outbound-interface name eth1
set icmp type 0
set icmp type 8
set action accept
commit
exit

NOTA: Recorda que el protocol ICMP (així com l'UDP) no incorporen el concepte de "connexió", així que el "truc" d'indicar l'estat "established" o "related" no funciona aquí. És per això que cal indicar tots els tipus de paquets ICMP explícitament tant en una direcció com en l'altra

* ¿Què fan cadascuna de les línies anteriors? ¿Funcionen ara els "pings" (fets tant des de la màquina real a la tarja *eth0* de la màquina VyOS com viceversa)? ¿Per què?

bV) ¿Per a què creus que serviria la següent regla executada al sistema VyOS?

configure
edit firewall ipv4 output filter rule 2
set tcp flags not syn
set action accept
commit
exit

bVI) Elimina totes les regles del tallafocs "filter" introduïdes en els anteriors apartats executant *delete firewall ipv4 ; commit* i comprova-ho (al mode operacional o de configuració, tant és) amb *show firewall*

Existeix una forma alternativa d'especificar les regles d'un tallafocs ni millor ni pitjor que la coneguda fins ara, simplement diferent (i que sovint és utilitzat quan el sistema tallafocs disposa de moltes tarjes de xarxa per la seva comoditat): la configuració "per zones". En aquesta forma, una "zona" s'associa a una determinada tarja de xarxa (i només a una; les tarjes de xarxa sí que es poden assignar a vàries zones, però) i el que es regula llavors és el tràfic que va d'una zona a una altra. En aquest cas, a la definició de les regles no s'indicaran les cadenes "input", "forward" o "output" sinó se'ls assignarà un determinat nom, que si és comú a diverses regles servirà per definir l'anomenat "ruleset". Aquest "ruleset" serà el que s'aplicarà al tràfic que vagi d'una determinada zona a una altra. Veiem-ho pas a pas:

1.-Assignar una zona, amb un nom determinat, a cada tarja de xarxa:

set firewall zone WAN interface eth0
set firewall zone LAN interface eth1

2.-Definir els diferents "rulesets", cadascun amb un nom determinat, una acció per defecte i les diferents regles que s'hi vulguin afegir. Per exemple:

set firewall name deDinsAFora default-action accept
set firewall name deForaADins default-action drop
set firewall name deForaADins rule 1 state established
set firewall name deForaADins rule 1 action accept
set firewall name deForaADins rule 2 protocol icmp
set firewall name deForaADins rule 2 action accept
set firewall name deForaADins rule 3 protocol tcp
set firewall name deForaADins rule 3 destination address 192.168.14.100
set firewall name deForaADins rule 3 destination port 80
set firewall name deForaADins rule 3 state new
set firewall name deForaADins rule 3 action accept

3.-Assignar el/s "ruleset/s" definits anteriorment al tràfic provinent d'una zona i dirigit a l'altra.

*De LAN a WAN: *set firewall zone WAN from LAN firewall name deDinsAFora*
*De WAN a LAN: *set firewall zone LAN from WAN firewall name deForaADins*

NOTA: Existeix per defecte una zona anomenada "**Local**" que representa el sistema VyOS en sí. Aquest zona és útil per encabir tot el tràfic que vagi dirigit o en surti al/del propi tallafocs (per exemple, de LAN->Local o WAN->Local, o de Local->LAN o Local->WAN, respectivament)
NOTA: Es pot comprovar la configuració general amb *show firewall zone-policy*

c) Explica amb les teves pròpies paraules quina serà la configuració final del sistema VyOS després d'aplicar els tres passos descrits als paràgrafs blaus anteriors, amb les comandes d'exemple que allà s'hi mostren

2.-a) ¿Quina funcionalitat oferta per VyOS és descrita en el següent apartat de la documentació oficial: https://docs.vyos.io/en/latest/configuration/service/conntrack-sync.html ?

b) ¿Quina funcionalitat oferta per VyOS és descrita en el següent apartat de la documentació oficial: https://docs.vyos.io/en/latest/configuration/trafficpolicy ?

D'altra banda, sense tenir a veure específicament amb l'àmbit de la gestió de tallafocs...

c) ¿Quina funcionalitat oferta per VyOS és descrita en el següent apartat de la documentació oficial: https://docs.vyos.io/en/latest/configuration/interfaces/wireguard.html? (un exemple d'implementació es troba a https://blog.kroy.io/2021/06/23/vyos-from-scratch-routing-and-vps-edition/#Home_Setup)

d) ¿Quina funcionalitat oferta per VyOS és descrita en el següent apartat de la documentació oficial: https://docs.vyos.io/en/latest/configuration/loadbalancing/reverse-proxy.html ?

e) ¿Quina funcionalitat oferta per VyOS és descrita en el següent apartat de la documentació oficial: https://docs.vyos.io/en/latest/configuration/interfaces/wireless.html ?

f) ¿Quina funcionalitat oferta per VyOS és descrita en el següent apartat de la documentació oficial: https://docs.vyos.io/en/latest/configuration/system/flow-accounting.html ?