Distribucions espacialitzades en Firewalling i més (UTMs)

Un UTM ("Unified Threat Management") és un dispositiu de seguretat que es col·loca a la xarxa i que incorpora habitualment funcionalitats de tallafocs, NAT, proxy TCP/HTTP (incloent filtres, catxé i/o balancejament), QoS i/o VPN, a més d'antivirus/antimalware/antiphishing/antispam/antiads, IDS i/o escàners de vulnerabilitats. També solen oferir altres serveis, per exemple de DNS, DHCP, sistemes d'accés a la xarxa basats en RADIUS/802.1X, o en LDAP amb RBAC ("role-based access control) o en mecanismes similars (en el que se'n diu específicament NAC -"Network Access Control"-) i/o implementació de sistemes "hotspot" (és a dir, de punts d'accés wifi), etc, etc, tot d'una forma unificada.

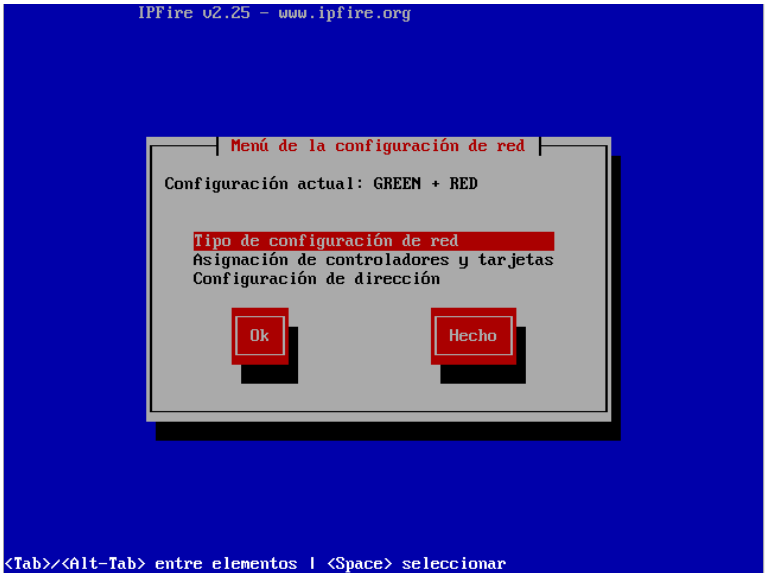
Tot i que hi ha maquinari específic per als UTM (podeu consultar els productes dels fabricants https://www.checkpoint.com o https://teklager.se -el qual proporciona hardware lliure!-, per exemple), també hi ha distribucions Linux o BSD especialment dissenyades per realitzar aquesta tasca i que poden instal·lar-se en un equip o màquina virtual estàndard. D'entre elles podem destacar:

*__IPFire__ (https://www.ipfire.org) -Basat en Linux però no depèn de cap distribució generalista-
*__OpenWRT__ (https://openwrt.org) - També basat en Linux i però tampoc en cap distribució general-
*__OPNSense__ (https://opnsense.org) -Basat en HardenedBSD-
*__PFSense__ (https://www.pfsense.org) -Basat en FreeBSD-
*__VyOS__ (https://vyos.io) -Ja el coneixem-
*__Packetfence__ (https://www.packetfence.org) -No és una distribució sinó un conjunt de software-

EXERCICIS:

1.-¿Què explica l'article https://teklager.se/en/best-free-linux-router-firewall-software-2019 ?

2.-a) Vés a https://www.ipfire.org/download i descarrega't la ISO d'IPFire. Crea una nova màquina virtual que tingui dues tarjes: la primera ha d'estar en mode xarxa interna" i la segona en mode "adaptador pont" (o també "NAT", tant se val). Arrenca aquesta màquina virtual amb la ISO d'IPFire i segueix tots els passos de l'assistent per instal·lar aquesta distribució al disc dur i també els de l'assistent del primer reinici fins arribar, en aquest darrer assistent, fins la pantalla de configuració de la xarxa, tal com aquesta:



b) En aquesta pantalla cal triar cadascuna de les tres opcions mostrades, una rera l'altra. A la primera ("Tipus de configuració de xarxa") caldrà triar la configuració que més s'avingui amb la infraestructura que tinguem; podem triar entre quatre possibilitats:

GREEN + RED : Tenim una xarxa interna (la "green") i una externa, connectada a l'ISP (la "red")
GREEN + RED + ORANGE : A més, tenim una DMZ (servidors propis públicament accessibles)
GREEN + RED + BLUE : Tenim una xarxa interna separada pels clients Wifi
GREEN + RED + ORANGE + BLUE : La combinació de totes les anteriors

> NOTA: Si s'usa la zona "Blue", es recomana assignar-la a una tarja Ethernet i llavors connectar aquesta a un punt d'accés separat. No obstant, és posible assignar la zona "Blue" directament a una tarja wifi del sistema sempre que es faci servir el addon "hostapd"

Tria l'opció "GREEN + RED". Tot seguit, caldrà assignar, amb l'opció "Asignació de controladors i tarjetes", cada zona de les indicades anteriorment a cadascuna de les tarjes de la màquina. Assigna la zona "RED" a la tarja en mode adaptador pont i la zona "GREEN" a la xarxa en mode xarxa interna. Finalment, vés a l'opció "Configuració de l'adreça" i assigna l'adreça 10.0.0.1/8 a la tarja "green" i una adreça via DHCP a la tarja "red". Un cop haguem establert aquestes tres opcions de la pantalla, podrem passar a la següent, on podem habilitar un servidor DHCP a la tarja "green"; fes-ho indicant un rang des de 10.0.0.100 fins la 10.0.0.150. I ja haurem acabat. El sistema s'autoreiniciarà de nou i apareixerà el login de terminal.

c) Al login gràfic indica l'usuari "root" i la contrasenya indicada durant la instal·lació. Un cop dins del sistema, executa les comandes *ip a* i *ip r* ¿Què veus? ¿Com es diuen les tarjes de xarxa? ¿I si executes *ps -ef*, quins processos pots reconèixer?

> NOTA: En qualsevol altre moment que es vulgui canviar alguna configuració de les introduïdes en els passos indicats a l'apartat anterior, només caldrà executar la comanda *setup* . La configuració del servidor DHCP es troba a "/etc/dhcp/dhcpd.conf"

d) Arrenca una segona màquina virtual amb la seva tarja de xarxa en mode "xarxa interna" i amb algun entorn gràfic. Confirma que hagi obtingut una IP del rang ofert per la màquina IpFire (amb *ip a*) i quina és la seva porta d'enllaç (amb *ip r)*. Confirma que tinguis accés a Internet (fent un simple "ping" a qualsevol IP i també nom DNS d'Internet...amb això estaràs comprovant que l'IP-Forward (i el "masquerading"!) està activat per defecte a l'IPFire).

e) Obre un navegador i vés a la URL https://10.0.0.1:444. Després d'acceptar l'excepció pel certificat autosignat, indica l'usuari "admin" i la contrasenya indicada durant la instal·lació. ¿Què veus finalment? Investiga les opcions del menú i digues tres funcionalitats que et semblin interessants típiques d'un UTM

f) Concretament, afegeix una regla de tallafocs que restringeixi amb una acció DROP l'accés des de la xarxa "green" a qualsevol port 5555/TCP escoltant a la xarxa "red" i aplica-la. Per provar-la, posa en marxa dos servidors Netcat a la màquina real escoltant respectivament al port 4444 i 5555, i comprova que des de la màquina virtual "client" pots accedir-hi perfectament al primer però no al segon.

fII) Modifica la regla de tallafocs anterior per a què ara restringeixi el mateix però amb una acció REJECT. Observa ara quin és el comportament del client quan es vol accedir de nou al port 5555. ¿Es diferent que a l'apartat anterior? ¿Per què? ¿Què passa si, finalment, desactives aquest regla i tornes a intentar connectar des del client al port 5555 de nou?

> NOTA: La documentació sobre com gestionar el tallafocs a IPFire es troba a https://wiki.ipfire.org/configuration/firewall i també a https://wiki.ipfire.org/configuration/firewall/nat

g) Vés al menú "IPFire->Pakfire" digues tres plugins que et semblin interessants d'instal·lar. En tens una llista a https://wiki.ipfire.org/addons

Molts dels "routers" oferits pels les empreses de telecomunicacions als seus clients particulars quan es donen d'alta del seu servei ISP venen, però, preinstal·lats pel NOS OpenWRT. Cal tenir en compte que aquests sistema (i altres similars com https://freshtomato.org) estan pensat per instal.lar-se en dispositius amb poca memòria, poca CPU i poc espai d'emmagatzematge. Per tant, cal tenir en compte les característiques del dispositiu en concret on realitzarem la instal.lació i comprovar si realment el sistema és compatible o no...perquè pot ser que no ho sigui (o calgui recompilar determinats mòduls del kernel per aconseguir-ho). En concret, la llista de hardware soportat pel sistema OpenWRT es pot consultar aquí: https://openwrt.org/toh, així que seria bona idea primer mirar en aquesta llista per veure quin dispositiu ens convé. No obstant, nosaltres ens descarregarem una imatge compatible amb un PC per posar-la en marxa en una màquina VirtualBox.

3.-a) Vés https://downloads.openwrt.org/releases/21.02.3/targets Allà es poden veure totes les arquitectures soportades per OpenWRT. Clica a l'enllaç "x86" i seguidament a l'enllaç " 64" per arribar a la pàgina de descàrregues pròpiament dita. Podem veure tenim diferents possibilitats:

*El fitxer "**generic-ext4-combined**" és un fitxer "raw" (és a dir, generat amb *dd* i "flasheable" igualment amb aquesta eina o similars, com *zcat imatge.img.gz > /dev/sdX*) que inclou un MBR amb el gestor d'arranc (Grub) que apunta a un kernel ubicat en una primera partició ext4 de 4MB, el qual arrenca la resta del sistema, que està ubicat en una segona partició ext4 de 48MB que conté tot el "rootfs". També està el fitxer "**generic-ext4-combined-efi**" que és equivalent a l'anterior però per sistemes UEFI, ja que inclou en comptes d'un MBR una partició EFI

NOTA: En qualsevol cas, s el nostre dispositiu oferís més espai d'emmagatezematge, sempre es pot fer més gran la segona partició o bé crear-ne de noves (i muntar-les automàticament a través de l'arxiu "/etc/fstab"

*El fitxer "**generic-squashfs-combined**" és similar a l'anterior però les particions són de tipus "squashfs" en comptes de "ext4". Aquest sistema es de només lectura, però en arrencar es munta un sistema de fitxers "overlay" a sobre de l'"squashfs" per poder fer canvis al sistema (només) durant el seu funcionament fins que s'apagui de nou (on tornarà a tenir la configuració original). També està el fitxer "**generic-squashfs-combined-efi**" que és equivalent a l'anterior però per sistemes UEFI, ja que inclou en comptes d'un MBR una partició EFI

*El fitxer "**generic-ext4-rootfs**" és un fitxer "raw" que conté només el "rootfs". Útil per "flashear" el seu contingut sobre una partició ext4 ja existent sense tocar el carregador d'arranc ni el kernel. És per això que tant se val que la màquina sigui BIOS o UEFI. També està el fitxer "**generic-squashfs-rootfs"**, similar a l'anterior però útil per "flashear" el seu contingut sobre una partició squashfs ja existent (sense tampoc tocar el carregador d'arranc ni el kernel). Igualment tenim el fitxer "**roofs**", él qual és un arxiu tar comprimit incloent només el "rootfs", útil per copiar el seu contingut sobre una partició/sistema de fitxers ja existent sense tocar el carregador d'arranc ni el kernel.

*El fitxer "**generic-kernel**" només és el kernel. Útil per copiar-lo directament a la seva partició corresponent si fos necessari per fallada/antiguitat del kernel actual.

NOTA: A més de l'enllaç de descàrrega del sistema pròpiament dit, cal tenir en compte també l'enllaç de descàrrega dels paquets que formen part de la distribució: https://downloads.openwrt.org/releases/21.02.3/targets/x86/64/packages (una llista més amigable es troba aquí https://openwrt.org/packages/start). Cal saber, en aquest sentit, que OpenWRT incorpora un gestor de paquets per línia de comandes anomenat "opkg" que és capaç de descarregar, instal.lar, desinstal.lar, comprovar, etc els paquets del sistema (a l'estil de l'*apt* de Debian o el *dnf* de Fedora).

b) Descarrega el fitxer "generic-ext4-combined-efi" de la versió més moderna actualment de OpenWRT, descomprimeix-lo amb la comanda *gunzip* i seguidament, converteix el fitxer ".img" resultant, ja descomprimit, en format VDI per a què el VirtualBox el pugui utilitzar com disc dur. Això es fa amb la comanda: *vboxmanage convertfromraw --format vdi nomfitxeractual.img nomfitxernou.vdi*

c) Crea una nova màquina virtual de tipus UEFI i assigna-li com a disc dur l'arxiu "vdi" creat a l'apartat anterior. Assigna-li també dues tarjes de xarxa: la primera ha d'estar obligatòriament en mode "xarxa interna" i la segona oblgatòriament en mode "adaptador pont" (o "NAT", tant se val).

NOTA: És important l'ordre en què establim els modes de les tarjes de xarxes, ja que la imatge ve amb una determinada configuració que cal respectar (no és com IPFire, on podíem triar quina era la tarja "green" i quina la "red"). Concretament, la tarja "eth0" (la primera pestanya del VirtualBox) està enllaçada amb una tarja "bridge" anomenada "br-lan" que automàticament per defecte **té la IP fixa 192.168.1.1** (això es podrà canviar). Aquesta tarja representa que és la que està al costat "LAN" del router. La raó del "bridge" és perquè allà també es vincularia, si existís, la tarja WiFi (normalment anomenada "wlan0") de tal forma que ambdues tarjes -la cablejada i la WiFi- serien totalment equivalents (de fet, tindrien la mateixa IP). En qualsevol cas, aquesta IP fixa és la que faríem servir per poder accedir al dispositiu des de qualsevol client via navegador/ssh per poder-lo configurar. D'altra banda, la tarja "eth1" (la segona pestanya del VirtualBox) representa que és la que està al costat "WAN" del dispositiu i és la que en donarà accés a Internet.

d) Arrenca aquesta màquina. Automàticament entraràs en una sessió de terminal de l'usuari "root" (per defecte no té contrasenya!). Executa les comandes *ip a* i *ip r* ¿Què veus? ¿Com es diuen les tarjes de xarxa? ¿Què significa que eth0 no tingui adreça IP però tingui associada la configuració *master br-lan*? ¿Què veus si executes *ps*, quins processos pots reconèixer? Assigna una contrasenya a l'usuari root amb la comanda *passwd*

NOTA: Els servidors DHCP (software *odhcpd* -integrat dins de *dnsmasq*- oferint per defecte IPs de la 192.168.1.100 a la 192.168.1.250) i el servidor HTTP (software *uhttpd* escoltant al port 80) estan activats al bridge br-lan però el servidor SSH (software *dropbear*) no està activat i el WiFi (en el cas de hardware que el suporti) estan apagats per seguretat.
NOTA: Les imatges per PCs estan configurades per usar tant comunicació sèrie (ttyS0,115200n8) com VGA; la majoria d'imatges de routers convencionals aquesta darrera opció no la tenen. Si es vol saber com serien els passos d'una instal.lació típica i d'accés posterior en un "router" sense pantalla (ni tanta CPU/memòria/emmagatzenament com el d'un PC) es pot llegir la guia "normal": https://openwrt.org/docs/guide-quick-start/start

e) Arrenca una segona màquina virtual amb la seva tarja de xarxa en mode "xarxa interna" i amb algun entorn gràfic. Confirma que hagi obtingut una IP del rang ofert per la màquina OpenWRT (amb *ip a*) i quina és la seva porta d'enllaç (amb *ip r)*. Confirma que tinguis accés a Internet (fent un simple "ping" a qualsevol IP i també nom DNS d'Internet...amb això estaràs comprovant que l'IP-Forward (i el "masquerading"!) està activat per defecte a l'OPenWRT).

f) Obre un navegador i vés a la URL http://192.168.1.1 ; indica l'usuari "root" i la contrasenya indicada durant la instal·lació. ¿Què veus finalment? Investiga les opcions del menú i digues tres funcionalitats que et semblin interessants típiques d'un UTM

g) Observa com, automàticament, OpenWRT ha assignat cada tarja a una "zona" del tallafocs (això ho pots comprovar anat al menú "Network"->"Interfaces"->"Edit"->"Firewall settings". Concretament, comprova que per defecte la tarja *br-lan* (on està inclosa *eth0*) està a la zona anomenada LAN (marcada de color verd) i la tarja eth1 està a la zona anomenada WAN (marcada de color vermell). Sabent això, vés al menú "Network"->"Firewall->"Traffic rules" i allà fes el necessari per afegir una regla de tallafocs que restringeixi amb una acció DROP l'accés des de zona LAN a qualsevol port 5555/TCP escoltant a qualsevol destí de la zona WAN, i aplica-la. Per provar-la, posa en marxa dos servidors Netcat a la màquina real escoltant respectivament al port 4444 i 5555, i comprova que des de la màquina virtual "client" pots accedir-hi perfectament al primer però no al segon.

gII) Modifica la regla de tallafocs anterior per a què ara restringeixi el mateix però amb una acció REJECT. Observa ara quin és el comportament del client quan es vol accedir de nou al port 5555. ¿Es diferent que a l'apartat anterior? ¿Per què? ¿Què passa si, finalment, desactives aquest regla i tornes a intentar connectar des del client al port 5555 de nou?

gIII) ¿Per a què serveix l'opció del menú "Network"->"Firewall"->"Port forwards" i com funciona?

h) Vés al menú "System"->"Software" digues tres plugins que et semblin interessants d'instal·lar.

OpenWRT ofereix una eina de terminal de comandes anomenada **uci** que serveix per administrar de forma centralitzada tots els elements del sistema; si bé es podrien utilitzar les utilitats bàsiques (comandes *ip*, etc) es recomana utilitzar aquesta eina perquè gestiona directament els arxius de configuració del sistema d'una manera homogènia. Aquests arxius de configuració són els que estan sota la carpeta "/etc/config" (com per exemple "network", "system", "dhcp", "uhttpd", "dropbear", "firewall" i "luci", entre altres).

NOTA: El panel de control web, que realitza la majoria de funcions similars a l'ein*a uci*, s'anomena **luci**

3BIS.-a) ¿Què és el que veus dins de l'arxiu "/etc/config/network"?

b) Canvia la IP fixa del bridge del sistema per a què en comptes de la que té (192.168.1.1) tingui la IP 10.0.0.1/8. Això ho podries fer editant directament l'arxiu anterior però també ho pots fer amb les següents comandes...:

uci show network
uci set network.lan.ipaddr='10.0.0.1'
uci set network.lan.netmask='255.0.0.0'
uci changes
uci commit
reboot (o bé *service network restart*)

NOTA: Altres comandes interessants (amb un significat evident) són, per exemple:
uci set network.lan.gateway='192.168.18.10' i *uci set network.lan.dns='8.8.8.8'*

...Després d'executar-les, comprova els canvis presents a l'arxiu "/etc/config/network"

c) Observa si cal que facis algun canvi dins de l'arxiu "/etc/config/dhcp", un cop canviada la IP del sistema OpenWRT, per a què a partir d'ara el servidor DHCP integrat concedeixi IPs al clients en el rang entre la 10.0.0.100 i la 10.0.0.250. En tot cas, reinicia el servidor DHCP d'OpenWRT amb la comanda *service odhcpd restart* i comprova, a la màquina client, que es rebi una IP del rang adient (pots fer simplement *sudo dhclient -r && sudo dhclient -v* per veure-ho).

NOTA: Pots apagar i deshabilitar el servidor DHCP d'OpenWRT executant, respectivament, les comandes *service odhcpd stop* i *service odhcpd disable*

d) Canvia, amb la comanda *uci set* ... adient, el nom del sistema OpenWRT a partir de la informació obtinguda de la sortida de la comanda *uci show system* i comprova que aquest canvi s'hagi guardat correctament dins del fitxer "/etc/config/system"

e) Canvia, amb la comanda *uci set* ... adient, el port d'escolta del servidor HTTP integrat al OpenWRT, a partir de la informació obtinguda de la sortida de la comanda *uci show uhttpd* i comprova que aquest canvi s'hagi guardat correctament dins del fitxer "/etc/config/uhttpd". Comprova també que pots seguir entrant al panell de control web des de la màquina client indicant ara el nou port d'escolta.

f) Comprova si el servidor SSH que ve per defecte a l'OpenWRT ("dropbear") està funcionant amb la comanda *service dropbear status* i intenta entrar des de la màquina client executant *ssh root@10.0.0.1* Atura aquest servidor i ara instal.la el servidor SSH "openssh-server" i posa'l en marxa en comptes del "dropbear"; això ho pots fer amb les següents comandes...:

opkg update
opkg install openssh-server
service sshd enable
Permet l'accés a "root" editant (amb *vi*) l'arxiu "/etc/ssh/sshd_config" per tenir la línia "PermitRootLogin yes"
service sshd start

...comprova tot seguit, executant *netstat -tln*, que a la màquina OpenWRT efectivament estigui el port 22 escoltant. Finalment, intenta accedir de nou al sistema OpenWRT via SSH des de la màquina client. ¿Què passa?

NOTA: Per saber més sobre *opkg*, consulteu https://lede-project.org/docs/user-guide/opkg

g) Executant *uci show firewall* (o bé, alternativament, llegint el contingut de l'arxiu "/etc/config/firewall"), dedueix quins ports -i en quina de les tarjes- estan tancats per defecte. ¿Quina relació té aquesta informació amb l'obtinguda del menú "Network"->"Firewall"->"Traffic rules". D'altra banda, ¿per a què serveix l'arxiu "/etc/firewall.user" i quina relació té amb el menú "Network"-"Firewall"->"Custom rules"?

NOTA: Per saber més sobre el tallafocs d'OpenWRT, consulteu https://openwrt.org/docs/guide-user/firewall/start