M11 – Seguretat Informàtica – UF1

Pràctica 2 Disseny de directives i IPTables_v04

Nil Massó

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

Table of Contents

• A l'hora d'avaluar i qualificar el treball es tindran en compte els aspectes estètics, de correctesa lingüística (sintàctica i ortogràfica) a més del que s'hagi comentat al cicle formatiu sobre la redacció de documentació tècnica i manuals.

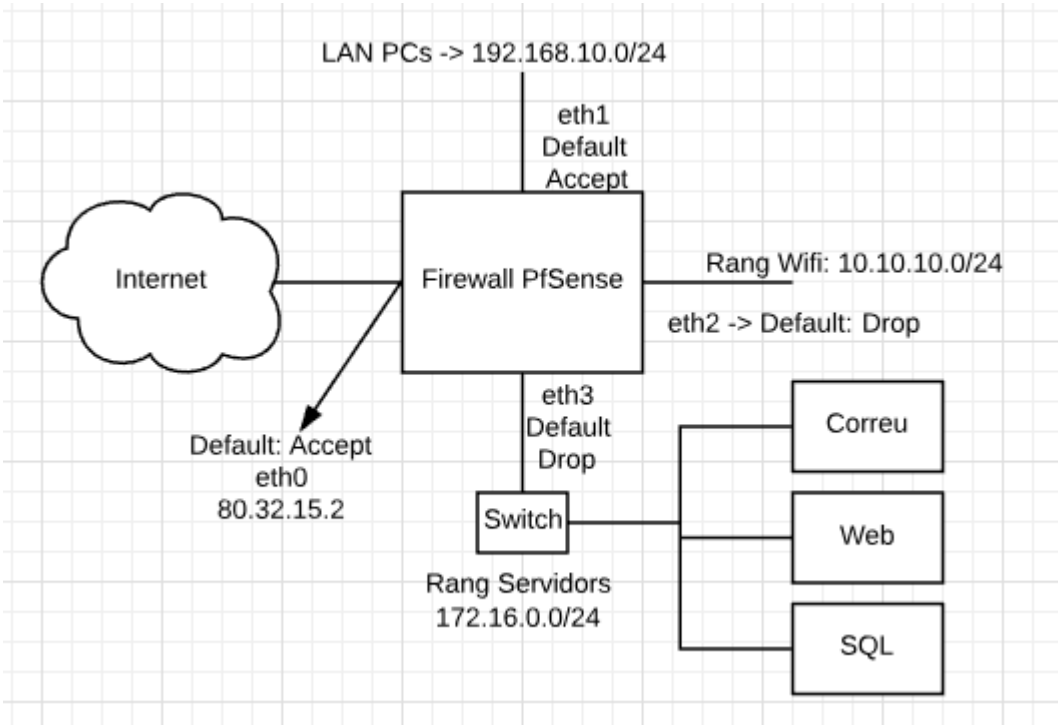
• El mòdul professional pertany a uns estudis orientats al món laboral, cosa que fa que un cop complerts els requisits mínims la nota resultant serà condicionada per la quantitat i qualitat del treball individual realitzat per cada alumne.

Pràctica 2 – Disseny de directives i IPTables

Exercici 1: Disseny de directives (2 + 3 punts)

1a part (2 punts)

Segons l'esquema adjunt i la informació addicional proporcionada cal traduir les expressions a '**llenguatge de firewall**', indicant IPs, ports, protocols i accions.



On heu de tenir en compte:
PC usuari1: 192.168.10.10
PC usuari2: 192.168.10.20
PC usuari3: 192.168.10.30
Wifi usuari4: 10.10.10.40
Wifi usuari5: 10.10.10.50

Servidor web: 172.16.0.100
Servidor correu: 172.16.0.200
Servidor MySQL: 172.16.0.150

Tingueu en compte que en aquest firewall **la política per defecte s'aplica a la ethernet tant pel trànsit entrant com sortint i que és statefull**.

Primer de tot us en proporciono un parell d'exemple per tal que entengueu què cal fer:

Regla A: Tot el rang de servidors pot anar a qualsevol lloc excepte la Wifi
Regla B: Tots els membres de Wifi poden navegar per servidors web d'Internet

Regla	interfície	Sentit	IP Origen	IP destí	Port origen	Port destí	Protocol	Acció
A	eth3	E	172.16.0.0/24	*	*	*	*	ACCEPT
B	eth2	E	*	*	*	80,443	TCP	ACCEPT

I aquí venen les que vosaltres heu de fer:

Regla 1: Bloquejar els enviaments de correu des de la LAN als servidors d'Internet
Regla 2: El port d'administració del firewall és el 8080, cal bloquejar l'accés al port des de Internet per qualsevol IP.
Regla 3: Els PCs de la LAN poden anar al moodle del servidor web (només per connexió segura)
Regla 4: Bloquejar que surtin pings a **Internet** de qualsevol equip inclòs el firewall
Regla 5: Permetre que el rang Wifi pugui fer servir la DNS de Cloudflare 1.1.1.1
Regla 6: Permetre que l'usuari5 pugui connectar amb el servei MySQL
Regla 7: Bloquejar que l'usuari3 pugui navegar a Internet tant per http com per https
Regla 8: Permetre que l'usuari4 pugui accedir a qualsevol PC de la LAN
Regla 9: Permetre que tota la LAN pugui fer ús del servidor de correu

Regla	Ethernet	Sentit	IP Origen	IP destí	Port origen	Port destí	Protocol	Acció
1	eth1	S	192.168.10.0/24	80.32.15.2	*	25	TCP	BLOCK
2	eth0	E	80.32.15.2	*	8080	8080	*	BLOCK
3	eth1	S	192.168.10.0/24	172.16.0.100	80	80	TCP	BLOCK
4	eth0	S	*	*	*	*	ICMP	BLOCK
5	eth2	S	10.10.10.0/24	1.1.1.1	*	53	UDP	ACCEPT
6	eth2	S	10.10.10.50	172.16.0.150	3306	3306	TCP	ACCEPT
7	eth0	S	192.168.10.30	*	80,443	80,443	*	BLOCK
8	eth2	S	10.10.10.40	192.168.10.0/24	*	*	*	ACCEPT
9	eth3	E	192.168.10.0/24	172.16.0.200	25	25	TCP	ACCEPT

2a part (3 punts)

Un cop teniu les directives dissenyades, **les heu de convertir al llenguatge o tipus de tallafoc** que feu servir. En aquesta pràctica les traduireu a **iptables**. Per tant, heu de generar les comandes corresponents.

Primer de tot us en proporciono un parell d'exemple per tal que entengueu què cal fer:

Regla A: Tot el rang de servidors pot anar a qualsevol lloc excepte la Wifi
Regla B: Tots els membres de Wifi poden navegar per Internet

Regla	Comanda
A	iptables -A FORWARD -i eth3 -s 172.16.0.0./24 -j ACCEPT
B	iptables -A FORWARD -i eth2 -p tcp –dport 80 -j ACCEPT

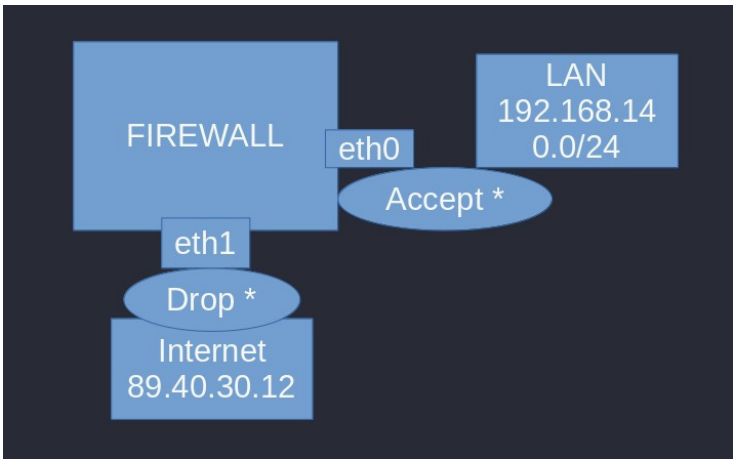
Empleneu la taula amb les comandes que heu de fer vosaltres:

Regla	Comanda
1	iptables -A FORWARD -i eth1 -o eth0 -s 192.168.10.0/24 -d 80.32.15.2 --dport 25 -p tcp -j DROP
2	iptables -A INPUT -i eth0 -s 80.32.15.2 -p tcp --dport 8080 -j DROP
3	iptables -A FORWARD -i eth1 -o eth0 -s 192.168.10.0/24 -d 172.16.0.100 -p tcp --dport 80 -j DROP
4	iptables -A OUTPUT -p icmp -j DROP
5	iptables -A FORWARD -i eth2 -o eth0 -s 10.10.10.0/24 -d 1.1.1.1 -p udp --dport 53 -j ACCEPT
6	iptables -A FORWARD -i eth2 -o eth0 -s 10.10.10.50 -d 172.16.0.150 -p tcp --dport 3306 -j ACCEPT
7	iptables -A FORWARD -i eth1 -o eth0 -s 192.168.10.30 -p tcp -m multiport --dports 80,443 -j DROP
8	iptables -A FORWARD -i eth2 -o eth1 -s 10.10.10.40 -d 192.168.10.0/24 -j ACCEPT
9	iptables -A FORWARD -i eth1 -o eth3 -s 192.168.10.0/24 -d 172.16.0.200 -p tcp --dport 25 -j ACCEPT

Exercici 2: Mapa de xarxa i Disseny de directives (5 punts)

Donada una arquitectura SOHO on vosaltres treballeu amb un PC dins la LAN, teniu un firewall amb 2 interfícies de xarxa (eth0 i eth1). La eth0 és la que dóna al costat LAN i la eth1 la que està a la part WAN i és qui té la IP pública pel que també ja fa de router cap a Internet.

a) **(2 punts)** Feu el dibuix del mapa de xarxa (semblant al de l'exercici 1) indicant la zona LAN i WAN, els noms de les interfícies de xarxa i marcar on s'apliquen les polítiques per defecte que són:
   - DROP a la eth1 (tant entrada com sortida)
   - ACCEPT a la eth0 (tant entrada com sortida)



A nivell de IPs. Inventeu-vos una IP pública per la vostra WAN i poseu-la també al mapa, i feu servir el vostre rang assignat a la taula següent per a definir les IPs de la part LAN posant **la .1 per al gateway i la que vulgueu pel PC**.

Cognom	Nom	Xarxa
Massó Cabañ,	Nil	192.168.140.0/24

b) Ompliu la següent taula de disseny de directives en "llenguatge de Firewall" genèric **(1,5 punts)**:
WAN: 80.32.15.2

Regla	Ethernet	Sentit	IP Origen	IP destí	Port origen	Port destí	Protocol	Acció
1	eth1	E	*	*	*	*	*	BLOCK
2	eth1	S	*	*	*	*	*	BLOCK
3	eth0	E	*	*	*	*	*	ACCEPT
4	eth0	S	*	*	*	*	*	ACCEPT
5								

Compte amb els protocols amb SSL (tipus http i https, per exemple)

Regles:

1) Permetre tot el correu SMTP de sortida per tal de poder enviar correus al nostre servidor de correu que està a Google (IP servidor 80.32.15.28)
2) Permetre tot el trànsit DNS des de la LAN a Internet
3) Bloquejar l'accés al Firewall des de la LAN sota HTTPs
4) Cal bloquejar l'accés a VPNs remotes (1194 UDP) pel PC que teniu a la LAN però permetre'l per la resta d'equips de la LAN si aquesta mai augmenta d'usuaris.
5) Permetre que els equips de la LAN es puguin connectar a servidors remots per a l'ús de FTP sota mode passiu (aquest pel port 6565) https://docs.cpanel.net/knowledge-base/ftp/how-to-enable-ftp-passive-mode/

c) Empleneu la taula amb les comandes corresponents de **iptables (1,5 punts)**:

Regla	Comanda
1	iptables -A FORWARD -i eth0 -o eth1 -s 192.168.10.0/24 -d 80.32.15.28 --dport 25 -p tcp -j ACCEPT
2	iptables -A FORWARD -i eth0 -o eth1 -s 192.168.10.0/24 -p udp --dport 53 -j ACCEPT
3	iptables -A FORWARD -i eth0 -o eth1 -s 192.168.10.0/24 -d 80.32.15.2 --dport 443 -p tcp -j DROP
4	iptables -A FORWARD -i eth0 -o eth1 -s 192.168.10.100 -p udp --dport 1194 -j DROP iptables -A FORWARD -i eth0 -o eth1 -s 192.168.10.0/24 -p udp --dport 1194 -j ACCEPT
5	iptables -A FORWARD -i eth0 -o eth1 -s 192.168.10.0/24 -p tcp --dport 6565 -j ACCEPT

d) (opcional) Si l'FTP de la regla 5 funcionés en mode actiu, creus que podries fer unes regles per-què funcionés? Si no pot funcionar, raona perquè no.

iptables -A FORWARD -i eth0 -o eth1 -s 192.168.10.0/24 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -s 192.168.10.0/24 -p tcp --dport 21 -j ACCEPT

e) (opcional) En cas que tinguessin un servei de SSH al nostre PC de LAN, podríem fer alguna/es regles per tal de que des de fora s'hi pogués accedir? Quines? En cas que no, perquè no?

iptables -A FORWARD -i eth1 -o eth0 -d 80.32.15.2 -p tcp --dport 22 -j ACCEPT
Jo no ho faria, molt perillos.