PROJECTE 2

SEGURETAT OPERACIONAL EMPRESARIAL

Curs: PQTM 19. Tècnic/a en Ciberseguretat

Ivan Ricart Borges iricartb@uoc.edu

ÍNDEX

1. CONFIGURACIÓ DE DOS TALLAFOCS EN UNA XARXA AMB DMZ

1.1. ESCENARI

Segons l'enunciat del projecte l'escenari ha de presentar tres zones de xarxa totalment diferenciades, xarxa interna, DMZ e Internet.

XARXA	DESCRIPCIÓ
A	La xarxa interna, on hi ha estacions de treball, amb adreçament 192.168.1.0/24 Adreçament: 192.168.1.1 - 192.168.1.254
Utilitzarem una direcció IPv4 del segment de la xarxa interna per permetre la configuració dels tallafocs, en aquest cas la **192.168.1.200**	
B	La DMZ, on hi ha un servidor web, amb adreçament 10.30.1.0/24 Adreçament: 10.30.1.1 - 10.30.1.254
L'enunciat no especifica la direcció IPv4 del servidor web, per tant, per resoldre el problema, li assignarem la direcció **10.30.1.1**	
C	Internet, amb adreça IP 80.19.234.55

Aquesta xarxa ha d'estar controlada amb dos tallafocs FW1 i FW2, on FW1 separa la zona C de la zona B i FW2 separa la zona B de la zona A. Els tallafocs tenen dues interfícies de xarxa, cadascuna amb la direcció IP corresponent a l'adreçament de la zona que li correspon.

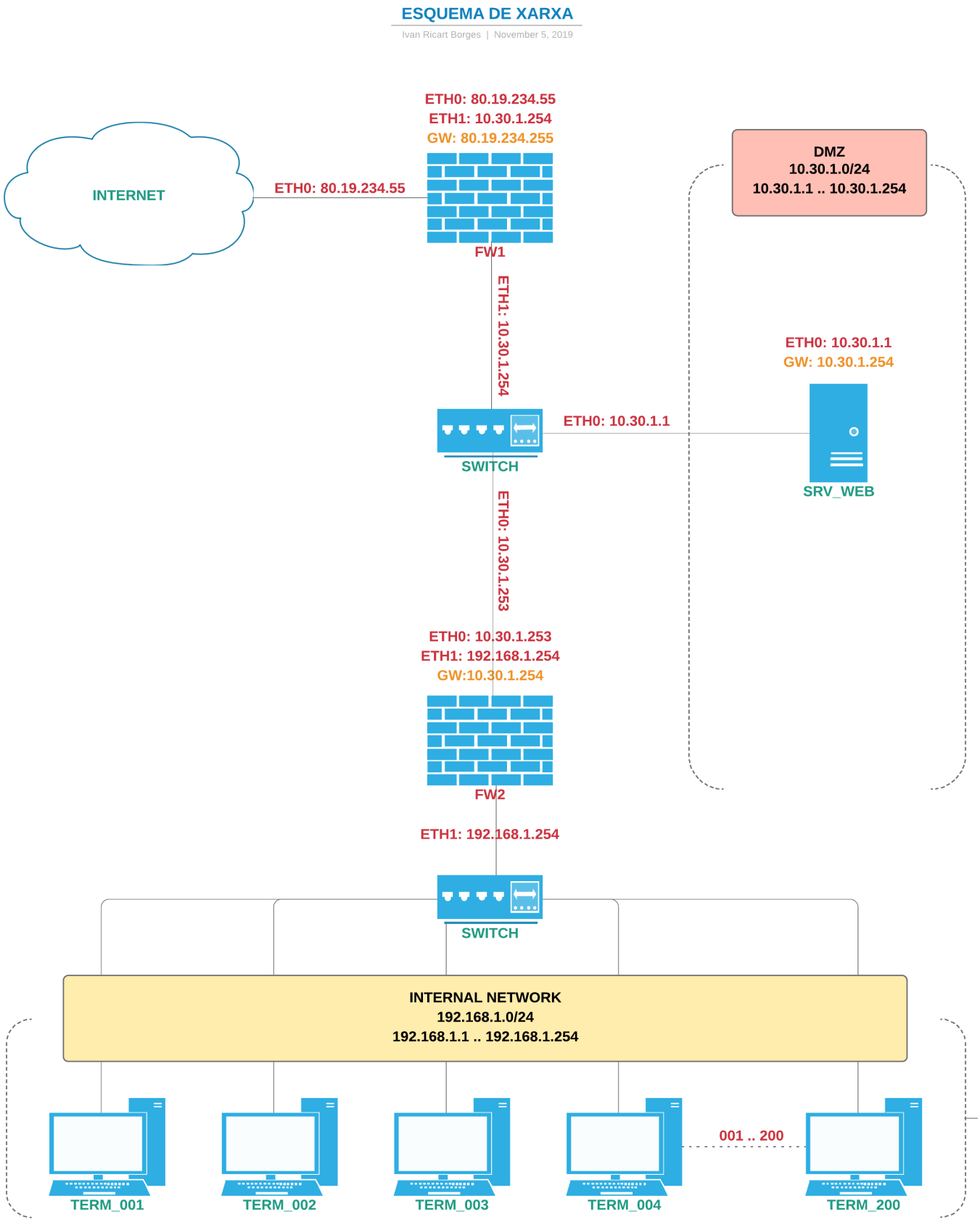
TALLAFOC	DESCRIPCIÓ
FW1	Separa la zona C de la zona B.
L'enunciat no especifica les direccions IPv4 de les dues interfícies de xarxa, per tant, per resoldre el problema, li assignarem les direccions **80.19.234.55** a la int. eth0 i **10.30.1.254** a la int. eth1.	
FW2	Separa la zona B de la zona A.
L'enunciat no especifica les direccions IPv4 de les dues interfícies de xarxa, per tant, per resoldre el problema, li assignarem les direccions **10.30.1.253** a la int. eth0 i **192.168.1.254** a la int. eth1.	

Les direccions IP privades assignades i que per tant no es podran utilitzar són les següents:

XARXA	DIRECCIONS IP
A	FW2: 192.168.1.254 (eth1), TERM_200: 192.168.1.200
B	FW1: 10.30.1.254 (eth1), FW2: 10.30.1.253 (eth0), SRV_WEB: 10.30.1.1
C	FW1: 80.19.234.55 (eth0)

1.2. ESQUEMA DE XARXA

A continuació es mostra la xarxa especificada anteriorment, mitjançant un esquema.



1.3. OBJECTIUS I CONFIGURACIÓ DELS TALLAFOCS

Segons l'enunciat s'han d'assolir una sèrie d'objectius, a continuació estudiarem cada un d'ells i les configuracions que s'han d'adoptar en els tallafocs.

OBJECTIU	CONFIGURACIÓ
Els usuaris de la zona A puguin navegar per Internet (HTTP, HTTPS, DNS).	Per permetre que els usuaris de la zona A puguin navegar per internet, s'hauran d'introduir regles al tallafoc [FW2] per permetre el tràfic web (80, 443) procedent de la zona A cap a la zona B, posteriorment, el tallafoc [FW1] reencaminarà la informació de la zona B cap a la zona C, en tots els casos es farà SNAT de la direcció IP origen.
Els usuaris de la zona A usen programari local per gestionar el correu. Han de poder usar un servidor IMAP i SMTP ubicat a la IP externa 85.113.19.44.	De forma anàloga al punt anterior, s'hauran d'introduir regles al tallafoc [FW2] per permetre el tràfic relacionat amb el correu electrònic (25, 143, 465, 587, 993) procedent de la zona A cap a la zona B, posteriorment, el tallafoc [FW1] reencaminarà la informació de la zona B cap a la zona C.
Els usuaris de la zona A no puguin rebre pings.	Les polítiques per defecte dels tallafocs seran de denegació, a més a més, les regles que s'introduiran al tallafoc [FW2] permetran que la informació d'origen viatgi de la zona A cap a la zona B, però no a la inversa.
El servidor de la DMZ pugui rebre peticions web tant de la zona A com de la zona C	Per permetre que els servidors de la DMZ puguin rebre peticions web des de la zona C, s'hauran d'introduir regles al tallafoc [FW1] per permetre el tràfic web (80, 443) i realitzar DNAT per redirigir el tràfic cap al servidor DMZ indicat, el tallafoc [FW2] també es veurà afectat per permetre la informació de la zona A cap a la zona B.
El servidor de la DMZ només es pugui gestionar amb SSH	De forma anàloga al punt anterior, s'hauran d'introduir regles al tallafoc [FW1] per permetre el tràfic relacionat amb el servei SSH (22) i realitzar DNAT per redirigir el tràfic cap al servidor DMZ indicat, el tallafoc [FW2] també es veurà afectat per permetre la informació de la zona A cap a la zona B.
El servidor de la DMZ ha no pot rebre més d'un 'ping' per segon	S'hauran d'introduir regles al tallafoc [FW2] per permetre el tràfic ICMP procedent de la zona A cap a la zona B, però amb una certa limitació per tema de seguretat.
Permetre connexió SSH als tallafocs	S'hauran d'introduir regles als tallafocs per permetre el tràfic relacionat amb el servei SSH (22), però en aquest cas, només acceptarem aquell tràfic procedent de la direcció IP 192.168.1.200.

1.4. REGLES DELS TALLAFOCS EN FORMA DE TAULA

Per assolir els objectius especificats anteriorment i facilitar la tasca de manteniment, s'han desenvolupat fitxers de script. A continuació es mostren les regles dels tallafoc FW1 amb forma de taula.

[FW1] TALLAFOC 1 - ZONA C I ZONA B
1. Configurar les dues interfícies de xarxa (eth0 i eth1): eth0: 80.19.234.55 eth1: 10.30.1.254
2. Configurar el gateway (gw) per poder encaminar els paquets cap a altres xarxes: gw: 80.19.234.254
3. Configurar el dispositiu com a gateway per permetre el reencaminament de paquets: ip_forward: 1
4. Resetejar totes les regles del tallafocs.
5. Establir una política per defecte de denegar tot el tràfic.
6. Configurar el tallafocs en mode stateful per acceptar automàticament les connexions de retorn.
7. Acceptar tot el tràfic procedent de la interfície localhost.
8. Configurar el tallafocs per fer SNAT, es a dir, modificar la direcció IP origen del paquets amb la establerta a la interfície eth0 per poder encaminar-los cap a Internet.
9. Acceptar tot el tràfic procedent de la Intranet i DMZ cap a Internet, però no a la inversa: eth1 ▸ eth0
10. Configurar el tallafoc per fer DNAT, es a dir, reencaminar els paquets destinats cap a un port especific cap a una direcció IP interna i un port, d'aquesta manera es permet la publicació dels serveis Web i SSH del servidor DMZ. eth0 ▸ eth1 IP: 10.30.1.1 Ports: 80, 443 i 22
11. Acceptar el tràfic procedent de Internet cap a la DMZ, es a dir, el tràfic del punt anterior. eth0 ▸ eth1 IP: 10.30.1.1 Ports: 80, 443 i 22
12. Acceptar el tràfic procedent del terminal 10.30.1.253 cap al servei SSH proporcionat pel FW1. eth1 ▸ eth0 (FW2 SNAT) ▸ eth1 (FW1) IP origen: 192.168.1.200 ▸ 10.30.1.253 (FW2 SNAT) IP destí: 10.30.1.254 Port: 22

A continuació es mostra el fitxer de configuració del tallafoc FW2.

[FW2] TALLAFOC 2 - ZONA B I ZONA A
1. Configurar les dues interfícies de xarxa (eth0 i eth1): eth0: 10.30.1.253 eth1: 192.168.1.254
2. Configurar el gateway (gw FW1) per poder encaminar els paquets cap a altres xarxes: gw: 10.30.1.254
3. Configurar el dispositiu com a gateway per permetre el reencaminament de paquets: ip_forward: 1
4. Resetejar totes les regles del tallafocs.
5. Establir una política per defecte de denegar tot el tràfic.
6. Configurar el tallafocs en mode stateful per acceptar automàticament les connexions de retorn.
7. Acceptar tot el tràfic procedent de la interfície localhost.
8. Configurar el tallafocs per fer SNAT, es a dir, modificar la direcció IP origen del paquets amb la establerta a la interfície eth0 per poder encaminar-los cap a la xarxa DMZ o Internet.
9. Acceptar el tràfic especificat, procedent de la Intranet cap a la DMZ e Internet. eth1 ▸ eth0 9.1 Acceptar el tràfic web. Ports: 80 i 443 9.2 Acceptar el tràfic DNS. Ports: 53 (tcp i udp) 9.3 Acceptar el tràfic SMTP i IMAP però només cap a la direcció IP pública 85.113.19.44. IP: 85.113.19.44 Ports: 25, 143, 465, 587 i 993 9.4 Acceptar el tràfic SSH cap al servidor de la DMZ. IP: 10.30.1.1 Port: 22
10. Acceptar el tràfic ICMP procedent de la Intranet cap a la DMZ, però amb limitació d'acceptació de paquets (1 paq / seg) i el tràfic ICMP de resposta de la DMZ cap a la Intranet. eth1 ▸ eth0 IP: 10.30.1.1 ICMP: 8 (ICMP Echo) i 0 (ICMP Echo Reply)
11. Acceptar el tràfic procedent del terminal 192.168.1.200 cap al servei SSH proporcionat pel FW2. IP: 192.168.1.200 Port: 22

1.5. REGLES DELS TALLAFOCS FENT ÚS DE L'EINA IPTABLES

Per assolir els objectius especificats anteriorment i facilitar la tasca de manteniment, s'han desenvolupat fitxers de script. A continuació es mostren les regles dels tallafoc FW1 fent ús de l'eina Iptables.

[FW1] TALLAFOC 1 - ZONA C I ZONA B

```
# Script de configuració del router/gateway/firewall (1)
# 1. Configurem les dues interfícies de xarxa (eth0 i eth1).
ifconfig eth0 80.19.234.55
ifconfig eth1 10.30.1.254

# 2. Indiquem al nostre gateway qui serà alhora el seu gateway/router (direcció IP del primer
#     router públic encarregat d'encaminar els paquets cap al destí, ex. 80.19.234.254).
route add default gw 80.19.234.254

# 3. Configurem el dispositiu com a gateway, permitent el reencaminament de paquets.
echo 1 > /proc/sys/net/ipv4/ip_forward

# 4. Resetejem les regles.
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

# 5. Especifiquem la política per defecte DROP.
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# 6. Configurem el tallafocs com stateful (ESTABLISHED, RELATED).
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
# 7. Acceptem tot el tràfic procedent de la interfície localhost.
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# 8. Fem SNAT sobre les sol·licituds de connexió a Internet procedents de la Intranet i DMZ.
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# 9. Acceptem el tràfic procedent de la Intranet i DMZ cap a Internet
#    Com que l'enunciat no especifica el tractament sobre el tràfic de sortida dels servidors de
#    la DMZ, aquests podran fer peticions cap a internet sense restricció.
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT

# 10. Fem DNAT sobre les sol·licituds rebudes per el gateway/firewall (1) procedents d'Internet
#       dirigides cap als serveis proporcionats per la DMZ (servidors públics), en aquest cas
#       els serveis de SSH i WEB.
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 22 -j DNAT --to 10.30.1.1:22
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 10.30.1.1:80
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to 10.30.1.1:443

# 11. Acceptem el tràfic procedent d'Internet dirigides cap als serveis proporcionats per la DMZ
#      (servidors públics), en aquest cas els serveis de SSH i WEB.
iptables -A FORWARD -i eth0 -o eth1 -d 10.30.1.1 -p tcp -m multiport
            --dport 22,80,443 -j ACCEPT

# 12. Acceptem el tràfic procedent del terminal 192.168.1.200 de la xarxa interna mitjançant el
#       servei SSH, per gestionar el gateway/firewall (1), degut a que aquesta xarxa ha de fer
#       SNAT amb la direcció IPv4 del gateway/firewall (2), hem d'acceptar la direcció IPv4
#       10.30.1.253.
iptables -A INPUT -s 10.30.1.253 -p tcp --dport 22 -j ACCEPT
```

A continuació es mostra el fitxer de configuració del tallafoc FW2.

[FW2] TALLAFOC 2 - ZONA B I ZONA A

```
# Script de configuració del router/gateway/firewall (2)
# 1. Configurem les dues interfícies de xarxa (eth0 i eth1).
ifconfig eth0 10.30.1.253
ifconfig eth1 192.168.1.254

# 2. Indiquem al nostre gateway qui serà alhora el seu gateway/router (en aquest cas hem
#     d'indicar la direcció IPv4 del FW1).
route add default gw 10.30.1.254

# 3. Configurem el dispositiu com a gateway, permitent el reencaminament de paquets.
echo 1 > /proc/sys/net/ipv4/ip_forward

# 4. Resetejem les regles.
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

# 5. Especifiquem la política per defecte DROP.
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# 6. Configurem el tallafocs com stateful (ESTABLISHED, RELATED).
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# 7. Acceptem tot el tràfic procedent de la interfície localhost.
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# 8. Fem SNAT sobre els paquets generats en la Intranet.
```

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# 9. Acceptem el tràfic especificat de la Intranet cap a la DMZ e Internet mitjançant el FW1
#    El tràfic contrari no es permet, per tant, una comunicació que s'origina en la DMZ cap a la
#    xarxa interna està prohibida, d'aquesta manera si un atacant pogués perpetrar un servidor
#    de la DMZ mitjançant una vulnerabilitat, els terminals de la xarxa interna estarien
#    protegits, d'aquí el motiu de l'existència d'una zona desmilitaritzada (DMZ).

#  9.1 Acceptem el tràfic procedent de la Intranet cap als serveis WEB.
iptables -A FORWARD -i eth1 -o eth0 -p tcp -m multiport --dport 80,443 -j ACCEPT

#  9.2 Acceptem el tràfic procedent de la Intranet cap als servei DNS.
iptables -A FORWARD -i eth1 -o eth0 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -p udp --dport 53 -j ACCEPT

#  9.3 Acceptem el tràfic procedent de la Intranet cap als serveis SMTP i IMAP de la direcció
#       IPv4 pública 85.113.19.44.
iptables -A FORWARD -i eth1 -o eth0 -d 85.113.19.44 -p tcp -m multiport --dport
25,143,465,587,993 -j ACCEPT

#  9.4 Acceptem el tràfic procedent de la Intranet cap al servei SSH del servidor
#       web de la DMZ.
iptables -A FORWARD -i eth1 -o eth0 -d 10.30.1.1 -p tcp --dport 22 -j ACCEPT

# 10. Acceptem el tràfic ICMP procedent de la Intranet cap al servidor DMZ amb protecció
#      contra atacs de denegació de servei, en aquest cas, es permet 1 paquet / segon
iptables -A FORWARD -i eth1 -o eth0 -d 10.30.1.1 -p icmp --icmp-type 8
            -m limit --limit 1/s -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -p icmp --icmp-type 0 -j ACCEPT

# 11. Acceptem el tràfic procedent del terminal 192.168.1.200 de la xarxa interna mitjançant el
#      servei SSH per gestionar el gateway/firewall (2).
iptables -A INPUT -s 192.168.1.200 -p tcp --dport 22 -j ACCEPT
```

2. OPINIÓ PERSONAL

La realització d'aquest treball m'ha permès ampliar els coneixements pràctics sobre la gestió d'una xarxa empresarial utilitzant mecanismes de seguretat de control de tràfic, he de reconèixer que el fet d'utilitzar dos tallafocs no ha sigut una tasca gens fàcil, l'esquema de seguretat es segmenta en àrees més específiques i en segons quins casos, aquests han d'estar ben coordinats per aconseguir els objectius que es persegueixen, personalment, crec que la dificultat de configuració és major que en el cas de configurar un sol tallafocs amb tres targetes de xarxa. També he de reconèixer que mai he tingut el plaer de configurar un tallafocs per una organització i crec que es una eina molt important per poder reduir la probabilitat d'ocurrència d'explotació de vulnerabilitats, controlant el tràfic es pot aïllar els problemes de tal manera, per exemple, que si algun usuari executa o s'introdueix un software malintencionat en algun terminal de la xarxa interna amb la capacitat de propagar-se, aquesta propagació podria aturar-se evitant la contaminació cap a altres terminals, per tant, crec que és una eina indispensable per tota organització i que ha d'estar correctament configurada.

3. FONTS D'INFORMACIÓ

Recursos

Recurs - Mecanismes de prevenció.
P07_05070_02623.pdf

Iptables

Manual pràctic de Iptables, tutorial pràctic i amb exemples. Pello Xabier Altadill Izurra.
https://www.scribd.com/document/336419815/IPTABLES-Manual-Practico-Tutorial-de-Iptables-Con-Ejemplos

Tècniques de defensa: Mecanismes comuns sota variants del sistema operatiu Linux.
https://www.scribd.com/document/7103092/Seguridad-Informatica-Tecnicas-de-defensa-comunes-bajo-variantes-del-sistema-operativo-Unix