# UD 4: "Instalación y configuración de cortafuegos"

## **CORTAFUEGOS:**

#### 1. CONFIGURACIÓN ROUTER-FIREWALL

Configura un router-firewall utilizando los simuladores correspondientes:

## a) Router DLINK:

Nos logueamos como administrador en el router.



Denegamos el rango de direcciones de la 2-100 y de la 101 a la 200, pero éste último los puertos desde el 80 al 110. Además tienen un control horario de 3:30 AM a 5:00 AM.



b) Router LINKSYS:

Podemos realizar un bloqueo de peticiones de anónimos, filtros multicast, filtrar el puerto 113 y un filtro de NAT.

LINKSYS® A Division of Cisco Systems, Inc.								Fim	ware Version : v4.30.0
						Wire	eless-G Broad	band Router	WRT54GL
Security	Setup	v	Vireless	Security	Access Restrictio	ns	Applications & Gaming	Administratio	n Status
	Firewall	1	VPN						
Firewall								Firewall Dr	otection : Enable
	Firev	wall Prot	ection : 🍳	Enable 🔘 D	isable			or disable th	ie SPI firewall.
Block WAN Requests	$\checkmark$	Block A	Anonymous I	nternet Request	3				
	<b>v</b>	Filter M	lulticast						
		Filter In	iternet NAT F	Redirection					
	$\checkmark$	Filter ID	DENT(Port 11	3)					
									CISCO SYSTEMS
				Sav	e Settings	Can	cel Changes		ավիտուդիրութ

Este router, sólo tiene la opción de habilitar y deshabilitar el firewall.

Firefox VD_04_SAD.pd	df (objeto application/p × 🗍 TL-WF	842ND ×	+			×	J
(+) www.tp-link.com/l	Resources/simulator/WR842ND(UN)1.0/	index.htm			☆ マ C Soogle	۸ 🌀 ۹	
M Gmail: correo electróni 竹 Cur	rsos de Inforactiva 🧯 AJ León, Valdep	eñas ( ) ( INTECO - Seguridad, I	💿 Miguel Ángel García F	🎿 Bienvenidos a la portada 😒	SecurityFocus 🔕 Como Configurar El D	» 🔝 Marcadore	s
TP-LINK	۲°				300Mbps Multi-Function V	Vireless N Router Model No. TL-WR842ND	The second se
Status Quick Setup WPS	Basic Security				Basic Security Help	ins on this page	
Network Wireless DHCP	Firewall SPI Firewall:	💿 Enable 💿 Disable			Firewall - Here you can enable or disable to SPI Firewall - Stateful Packet Inspec cyber attacks by tracking more stat that the traffic passing through the	he Router's firewall. ction (SPI) helps to prevent te per session. It validates e session conforms to the	
VPN USB Settings Forwarding Security Basic Security - Advanced Security	VPN PPTP Passthrough: L2TP Passthrough: IPSec Passthrough:	<ul> <li>enable</li> <li>Disable</li> <li>Enable</li> <li>Disable</li> <li>Enable</li> <li>Disable</li> </ul>			protocol. SPI Firewall is enabled b all the computers on the LAN exp you can disable it. VPN - VPN Passthrough must be enable tunnels using VPN protocols to pass throu • PPTP Passthrough - PPTP P; Tunneling Protocol (PPTP) allows	/ factory default. If you want osed to the outside world, d if you want to allow VPN gh the Router. assthrough. Point-to-Point the Point-to-Point Protocol	
Local Management     Local Management     Remote Management     Parental Control     Access Control     Advanced Routing     Bandwidth Control     IP & MAC Binding     Dynamic DNS     System Tools	ALG FTP ALG: TTTP ALG: H323 ALG: RTSP ALG:	Enable Disable     Enable Disable     Enable Disable     Enable Disable     Enable Disable     Save			<ul> <li>(PPP) to be tunneled through an tunnels to pass through the Router,</li> <li>(2TP Passthrough - Layer Two T</li> <li>the method usad to enable Point Internet on the Layer Two level. To through the Router, citck Enable.</li> <li>IPSec Passthrough - Internet Prosult of protocols for en communications over Internet Prot the use of cryptographic security tunnels to pass through the Router,</li> <li>ALG - It is recommended to enable Apolic because ALG allows customized Network traversal filters to be plugged into the gates.</li> </ul>	P network To allow PPTP cickEnable. Inneling Protocol (L2TP) is to-Dorit sessions via the allow L2TP tunnels to pass tocol security (IPSec) is a suring private, secure col (IP) networks, through services. To allow IPSec cick Enable. atlon Layer Gateway (ALG) Address Translation (NAT) way to support address and yer 'control/date' protocols -	

- 2. ACL (CISCO)
- a) Resolución de ejercicios.
- b) Resolución escenario UD3-2.a. Router Frontera.



#### Uso de ACL estándar:

1) Elige el router adecuado para que los paquetes del PC1 no sean transmitido por la red 10.XX.0.0. Comprobar que si se permite los

RNORTE	
Physical Config CLI	
IOS Command Line Interface	
Sending 3, 100-byte Tomp Lends to 198.2.0.10, timebut 19.2 Seconds. .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 5/7/10 ms	*
<pre>RNORTE‡conf t Enter configuration commands, one per line. End with CNTL/Z. RNORTE(config)‡access-list 1 deny host 196.2.0.10 RNORTE(config)‡access-list 1 permit any RNORTE(config)‡interface FastEthernet 0/0 RNORTE(config-if)‡ip access-group 1 in RNORTE(config-if)‡ RNORTE(config-if)‡ RNORTE(config-if)‡</pre>	
<pre>%SYS-5-CONFIG_I: Configured from console by console RNORTE#copy running-config startup-config Destination filename [startup-config]? Building configuration [OK]</pre>	
<pre>RNORTE#ping 196.2.0.10 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 196.2.0.10, timeout is 2 seconds: Success rate is 0 percent (0/5)</pre>	III I
Сору	Paste

Comprobamos que el PC2 puede mandar paquetes al RSUR



Sin embargo si hacemos lo mismo con el PC1 no permite mandar paquetes.



2) Configurar en la red 192.XX.0.0/24 un filtro "anti-spoofing" para que no sea enviado ningún paquete por la red 10.XX.0.0 que no coincida con su dirección de origen. Realizarlo también para la red 196.XX.0.20

Configuramos las acl para la IP 196.2.0.20.

RNORTE		-	_	
Physical	Config	CLI		
			IOS Command Line Interface	
				*
Press RE	TURN to g	et sta:	rted.	
RNORTE>e	nable			
Enter co	nfiguratio	on com	mands, one per line. End with CNTL/Z.	
RNORTE (C RNORTE (C	onfig) #ac	cess-l: cess-l:	ist 2 deny host 196.2.0.20 ist 2 permit anv	
RNORTE (c	onfig) #in	terface	= FastEthernet 0/0	E
RNORTE (c	onfig-if)	tip aco	cess-group 2 in	
KNOKIE (C	Unitig-11)	•		
				Copy Paste



Configuramos las acl para la IP 196.2.0.2.

Physical Config CLI IOS Command Line Interface \$5YS-5-CONFIG_I: Configured from console by console BNORTE#confy running-config startup-config Destination filename [startup-config]? Building configuration [OK] RNORTE#config t Enter configuration commands, one per line. End with CNTL/2. RNORTE@config t 3 deny host 196.2.0.2	
IOS Command Line Interface \$\$Y\$-5-CONFIG_I: Configured from console by console RNORTERcopy running-config startup-config Destination filename [startup-config]? Building configuresion [OK] RNORTE#config t Enter configuration commands, one per line. End with CNTL/2. RNORTE#config t 3 deny host 196.2.0.2	
<pre>\$SYS-5-CONFIG_I: Configured from console by console NNORTE#copy running-config startup-config Destination filemame [startup-config]? Building configuration [OK] NNORTE#config t Enter configuration commands, one per line. End with CNTL/Z. NNORTE#config taccess-list 3 deny host 196.2.0.2</pre>	
<pre>RNORTE(config)#access-list 3 permit any RNORTE(config)#interface FastEthernet 0/0 RNORTE(config-if)#ip access-group 3 in RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)# RNORTE(config-if)#</pre>	
Сору	Paste

SERVNORTE	- • ×
Physical Config Desktop Software/Services	
Command Prompt	X
Pinging 196.2.0.20 with 32 bytes of data:	<b>^</b>
Reply from 196.2.0.20: bytes=32 time=8ms TTL=128	
Reply from 196.2.0.20: bytes=32 time=6ms TTL=128	
Reply from 196.2.0.20: bytes=32 time=8ms TTL=128	
Reply from 196.2.0.20: bytes=32 time=9ms TTL=128	
Ping statistics for 196.2.0.20:	
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),	
Approximate round trip times in milli-seconds:	
Minimum = 6ms, Maximum = 9ms, Average = 7ms	
SERVER>ping 192.2.0.2	
Pinging 192.2.0.2 with 32 bytes of data:	=
Reply from 196.2.0.1: Destination host unreachable.	
Reply from 196.2.0.1: Destination host unreachable.	
Reply from 196.2.0.1: Destination host unreachable.	
Reply from 196.2.0.1: Destination host unreachable.	
Ping statistics for 192.2.0.2:	
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),	
SERVER>	-

En la red 192.2.0.0:

#### Configuramos las acl para la IP 192.2.0.10

RSUR		3
Physical Config CLI		
IOS Command Line Interface		
RSORFCOPY running-config startup-config		n U
Destination filename [startup-config]?	·	
Building configuration		
[OK]		
RSUR#		11
RSUR#		11
RSUR#		
RSUR#		11
RSUR#config t		11
Enter configuration commands, one per line. End with CNTL/Z.		11
RSUR(config) #access-list 1 deny host 192.2.0.10		11
RSUR(config) #access-list 1 permit any		11
RSUR(config) #interface FastEthernet 0/0		11
RSUR(config-if) #ip access-group 1 in		11
RSUR(config-if)#		11
RSUR(config-if)#		11
RSUR(config-if) #end		
SYS-5-CONFIG I: Configured from console by console		
RSUR#copy running-config startup-config		11
Destination filename [startup-config]?		
Building configuration	=	
[OK]	1	
RSUR#	-	
	Conv	ה
	Copy Paste	



Configuramos las acl para la IP 192.2.0.20

RSUR	
Physical Config CLI	
IOS Command Line Interface	
RSDR(CONFIG=11)+	*
kaok(conrig-ir)‡end	
<pre>%SYS-5-CONFIG_I: Configured from console by console</pre>	
RSUR#copy running-config startup-config	
Destination filename [startup-config]?	
Building configuration	
BSUB#config t	
Enter configuration commands, one per line. End with CNTL/Z.	
RSUR(config) #access-list 2 deny host 192.2.0.20	
RSUR(config) #access-list 2 permit any	
RSUR(config) #interface FastEthernet 0/0	
RSUR(config-if) #ip access-group 2 in	
RSUR(config=1f)#	
BSUB (config-if) #end	
%SYS-5-CONFIG_I: Configured from console by console	
RSUR#copy running-config startup-config	
Destination filename [startup-config]?	
Building configuration	=
	-
	Copy Paste



Configuramos las acl para la IP 192.2.0.2

Physical Config         CLI           IOS Command Line Interface           IVX:           BSUB#config t         Enter configuration commands, one per line. End with CNTL/Z.           RSUB (config) #         RSUB (config) #	
IOS Command Line Interface	Physical Config CLI
TOR/ RSUB/config t       *         RSUB/config t       Enter configuration commands, one per line. End with CNTL/Z.         RSUB(config) #       RSUB(config) #         RSUB	IOS Command Line Interface
<pre>RSUR(config)#access-list 2 permit any RSUR(config)#access-list 3 permit any RSUR(config)#interface FastExternet 0/0 RSUR(config)#interface FastExternet 0/0 RSUR(config-if)#access-group 3 in RSUR(config-if)#and RSUR[ RSUR[Config-if)#and RSUR[ SSUR[</pre>	10x1       *         SUB#config t       *         Enter configuration commands, one per line. End with CNTL/2.       #         RSUB(config) #       #         R
RSUR#    Copy Paste	RSUR#    Copy Paste

Comprobamos los resultados.



3) Borrar las ACLs definidas anteriormente.

#### Router Norte:

RNORTE	Caral a ferration of the local	
Physical Config CLI		
	IOS Command Line Interface	
RNORTE>enable RNORTE:config t Enter configuration comm RNORTE(config) for access RNORTE(config) fo	mands, one per line. End with CNTL/Z. list 1 list 2 list 3 ured from console by console tup-config actup-config]? 	× ×
		Copy Paste

Router Sur:

RSUR	
Physical Config CLI	
IOS Command Line Interface	
<pre>SUDE(config+if)#j=access-group 2 in SEUE(config+if)#j=access-group 2 in SEUE(config+if)# SEUE(config+if)#and ASUS-5-CONFIG_I: Configured from console by console SEUE(config)#and Bestination filename [startup-config] Bestination filename [startup-config]? Building configuration commands, one per line. End with CNTL/Z. RSUE(config)#no access-list 1 RSUE(config)#no access-list 1 RSUE(config)#no access-list 3 RSUE(config)#no access-list 3 RSUE(config)#no access-list 3 RSUE(config)#no RSUE(config)#no RSUE(config)#end SSUE(confi</pre>	
IOR) RSUR#	+
	Copy Paste

#### Uso de ACL COMPLEJAS

4) Permitir que el equipo PC3 pueda utilizar el servidor HTTP de SERVNORTE y no pueda utilizar el resto de servicios de dicho servidor.

RSUR	
Physical Config CLI	
IOS Command Line Interface	
REOR(CONTIG):	
RSUR (config) #	
RSUR (config) #	
RSUR (config) #	
RSUR(config) #	
RSUR (config) #	
RSUR(conrig) #	
RSUR (config) #	
RSUR(config)*	
RSUR(config) faccess-list 101 deny vdp host 192.2.0.10 host 196.2.0.2 eq 2	
DSUD (config) access list 101 days day have any	
DSUB (config) taccase list 101 permit udp any any	
PSUD (config) finterface fa0/0	
RSUR(config-if) #ip access-group 101 in	
RSUR(config-if) #	
RSUR (config-if) #end	
\$SYS-5-CONFIG_I: Configured from console by console	
RSUR#copy running-config startup-config	
Destination filename [startup-config]?	=
Building configuration	
[OK]	
RSUR#	*
	<b>D</b>
Сору	Paste

5) Permitir que el equipo PC1 pueda utilizar el servidor FTP de SERVSUR y el PC2 no pueda utilizarlo dicho servicio.

Configuramos en el router NORTE, para agregar las ACLs.



Comprobamos que PC1 puede acceder vía FTP de SERVSUR



Comprobamos que el PC2 no puede acceder.

PC2	
Physical Config Desktop	Software/Services
Command Prompt	X
PC>	A
PC>	
DC>	
PC>	
PC>	
PC>ftp 192.2.0.2	
Trying to connect192.2.0	.2
%Error opening ftp://192.2.	0.2/ (Timed out)
•	
Packet Tracer PC Command Li	ne 1 0
PC>(Disconnecting from ftp	server)
Packet Tracer PC Command Li	he 1.0
PC>	·
L	

6) No permitir que el PC2 pueda comunicarse con el PC4.

RNORTE	- 0 <b>X</b>
Physical Config CLI	
IOS Command Line Interface	
RNORTE(config-if); ENORTE(config-if);	*
\$SYS-5-CONFIG_I: Configured from console by console	
RNORTE‡copy running-config startup-config	
Destination filename [startup-config]?	
Building configuration	
[OK]	
RNORTE‡config t	
Enter configuration commands, one per line. End with CNTL/Z.	
RNORTE (config) #	
RNORTE (config) #	
RNORTE(config) #access-list 103 deny icmp host 196.2.0.2 host 192.2.0.2	
RNORTE(config) #interface fa0/0	
RNORTE(config-if) #ip access-group 103 in	
RNORTE (config-if) #	
RNORTE (config-if) #end	
%SYS-5-CONFIG_I: Configured from console by console	
RNORTE#copy running-config startup-config	
Destination filename [startup-config]?	
Building configuration	=
[OK]	
RNORTE#	*
Сору	Paste

Comprobamos que ya no podemos acceder a PC4 desde PC2.



#### 7) Borrar las ACLs anteriores.

Borramos las ACLs.

RNORTE		and the second second second	
Physical Config	CLI		
		IOS Command Line Interface	
PNOPTE (config) #	con com	ands, one per line. End with CWID/2.	*
RNORTE (config) #			
RNORTE (config) #n	acces	-list 101	
RNORTE (config) #n	acces	-list 102	
RNORTE (config) #n	acces	-list 102	
RNORTE (config) #n	acces	-list 103	
RNORTE (config) #i:	nterfac	fa0/0	
RNORTE (config-if	#no ip	access-group 101 in	
RNORTE (config-if	#no ip	access-group 102 in	
RNORTE (config-if	‡no ip	access-group 103 in	
RNORTE (config-if	) #		
RNORTE (config-if	tend \$		
SYS-5-CONFIG_I:	Config	red from console by console	
RNORTE#copy runn	ing-con	ig startup-config	
Destination file:	name [s	artup-config]?	
Building configu	ration.		=
[OK]			
RNORTE#			-
			Copy Paste

8) No permitir que los ordenadores de la red 192.XX.0.0 se comuniquen con los ordenadores de la red 196.XX.0.0

🥐 RNORTE
Physical Config CLI
IOS Command Line Interface
DNODTF (config) #
RNORTE (config) #
RNORTE (config) #
RNORTE (config) #
RNORIE (config) #
RNORTE (config) #
RNORTE (config) #
RNORTE (config) #
RNORTE(config) #access-list 101 deny tcp 192.2.0.0 0.0.0.255 196.2.0.0 0.0.0.255
RNORTE(config) #access-list 101 deny icmp 192.2.0.0 0.0.0.255 196.2.0.0 0.0.0.255
RNORTE (config) #interface fa0/0
RNORTE(config-if) #ip access-group 100 in
RNORTE(config-if)#ip access-group 101 in
RNORTE(config-if) #
RNORTE(config-if) #end
RNORTE#
SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Sullaing configuration
NIVA184
Copy Paste

Comprobamos el resultado



9) Borrar las ACL definidas anteriormente.

```
RNORTE(config)#
RNORTE(config)#no access-list 101
RNORTE(config)#
```



10) Impedir cualquier tráfico ICMP entrante excepto el "Destino Unreachable" y el "Echo Reply" en el router RNORTE.

## 3. IPTABLES (LINUX)a) Resolución de ejercicios

1º) Ver la versión de Iptables:

```
root@miguel:/home/miguel# iptables -V
iptables v1.4.4
root@miguel:/home/miguel#
```

2º) Borrado de todas las reglas

```
root@miguel:/home/miguel# iptables -F
root@miguel:/home/miguel# iptables -X
root@miguel:/home/miguel# iptables -Z
root@miguel:/home/miguel# iptables -t nat -F
root@miguel:/home/miguel#
```

3º) Añadir una regla a la cadena INPUT para aceptar todos los paquetes que se originan desde la dirección 192.168.0.155.

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.0.155 -j ACCEPT
root@miguel:/home/miguel# iptables -L
Chain INPUT (policy ACCEPT)
target
        prot opt source
                                        destination
ACCEPT
          all -- 192.168.0.155
                                        anywhere
Chain FORWARD (policy ACCEPT)
                                        destination
target
          prot opt source
Chain OUTPUT (policy ACCEPT)
                                        destination
target
          prot opt source
root@miguel:/home/miguel#
```

Comprobamos.

C:\Documents and Settings>ping 192.168.0.10 Haciendo ping a 192.168.0.10 con 32 bytes de datos: Respuesta desde 192.168.0.10: bytes=32 tiempo=4ms TTL=64 Respuesta desde 192.168.0.10: bytes=32 tiempo<1m TTL=64 Respuesta desde 192.168.0.10: bytes=32 tiempo<1m TTL=64 Respuesta desde 192.168.0.10: bytes=32 tiempo<1m TTL=64 Estadísticas de ping para 192.168.0.10: Paquetes: enviados = 4, recibidos = 4, perdidos = 0 <0% perdidos>, Tiempos aproximados de ida y vuelta en milisegundos: Mínimo = Øms, Máximo = 4ms, Media = 1ms C:\Documents and Settings>

4º) Eliminar todos los paquetes que entren.

```
root@miguel:/home/miguel# iptables -A INPUT -j DROP
root@miguel:/home/miguel#
```

5º) Permitir la salida de paquetes.

```
root@miguel:/home/miguel# iptables -A OUTPUT -j ACCEPT
root@miguel:/home/miguel#
```

6<sup>o</sup>) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155.

7º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección de red 192.168.0.0.



8º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155 y enviar un mensaje de error icmp.

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.0.155 -j REJECT
root@miguel:/home/miguel#
```

9º) Permitir conexiones locales (al localhost), por ejemplo a mysql.



10º) Permitir el acceso a nuestro servidor web (puerto TCP 80).

```
root@miguel:/home/miguel# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@miguel:/home/miguel#
```

11º) Permitir el acceso a nuestro servidor ftp (puerto TCP 20 y 21).

```
root@miguel:/home/miguel# iptables -A INPUT -p tcp --dport 20 -j ACCEPT
root@miguel:/home/miguel# iptables -A INPUT -p tcp --dport 21 -j ACCEPT
root@miguel:/home/miguel#
```

12<sup>a</sup>) Permitimos a la máquina con IP 192.168.0.155 conectarse a nuestro equipo a través de SSH.

13º) Rechazamos a la máquina con IP 192.168.0.155 conectarse a nuestro equipo a través de Telnet.

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.0.10 -p tcp --dport 23 -j
DROP
root@miguel:/home/miguel#
```

14º) Rechazamos las conexiones que se originen de la máquina con la dirección física 00:db:f0:34:ab:78.

```
root@miguel:/home/miguel# iptables -A INPUT -M 00:0c:29:de:dd:33 -i REJECT
root@miguel:/home/miguel#
```

## Firewall de una LAN



15º) Rechazamos todo el tráfico que ingrese a nuestra red LAN 192.168.0.0 /24 desde una red remota, como Internet, a través de la interfaz eth0.



16º) Cerramos el rango de puerto bien conocido desde cualquier origen:



17<sup>o</sup>) Aceptamos que vayan de nuestra red 192.168.0.0/24 a un servidor web (puerto 80):

```
root@miguel:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -p tcp -
-dport 80 -j ACCEPT
root@miguel:/home/miguel#
```

18º) Aceptamos que nuestra LAN 192.168.0.0/24 vayan a puertos https:



19<sup>o</sup>) Aceptamos que los equipos de nuestra red LAN 192.168.0.0/24 consulten los DNS, y denegamos todo el resto a nuestra red:

```
root@miguel:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -p tcp -
-dport 53 -j ACCEPT
root@miguel:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -p udp -
-dport 53 -j ACCEPT
root@miguel:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -j DROP
root@miguel:/home/miguel#
```

20º) Permitimos enviar y recibir e-mail a todos:



21º) Cerramos el acceso de una red definida 192.168.3.0/24 a nuestra red LAN 192.168.2.0/24:

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.3.0/24 -d 192.168.0.0/24
-j DROP
root@miguel:/home/miguel#
```

22<sup>o</sup>) Permitimos el paso de un equipo específico 192.168.3.5 a un servicio (puerto 5432) que ofrece un equipo específico (192.168.0.5) y su respuesta:



23º) Permitimos el paso de paquetes cuya conexión ya se ha establecido o es nueva pero está relacionada a una conexión ya establecida.

## b) Resolución escenario UD3-1.a. NAT.

#### 192.168.2.151 192.168.2.150 PC-PT 10.33.2.70 10.33.2.1 XP 2950-24 NAT EXTERIOR 2950-24 PC-PT PC-PT VNET2 Ubuntu Desktop Ubuntu Server LAN

#### Escenario

Establecemos la iptable, para que todo lo que salga por la interfaz eth1 salga por la eth0.

🔲 Ubuntu Server - VMw	vare Workstation	
File Edit View V	/M Team Windows Help	
🗖 II 🗋 🗐 🚺	🖄 🕼 🚺 🖬 🖬 🖬 🕞 🔛 🔤 🚺 🚯 👘	
Sidebar ×	🚰 ws2003_1 🗙 🔓 Ubuntu_Desktop 🗙 👘 Windows XP Pro	offesional 1 🗙 🔐 Ubuntu Server 🗙
Powered On     On     Ubuntu_Desk     Windows XP     Ubuntu Serve     Dubuntu Serve	root@equipo02:/# iptables -t nat -F root@equipo02:/# iptables -t nat -X root@equipo02:/# iptables -t nat -Z root@equipo02:/# iptables -t nat -L -n Chain PREROUTING (policy ACCEPT)	
Ubuntu_Desk	target prot opt source	destination
	Chain OUTPUT (policy ACCEPT) target prot opt source	destination
	Chain POSTROUTING (policy ACCEPT) target protopt source root@equipo02:/# iptables -t nat -A POST 168.2.150 root@equipo02:/# iptables -t nat -L -n Chain PRERDUITING (nolicu ACCEPT)	destination ROUTING -o eth1 -j SNATto-source 192.
	target prot opt source	destination
	Chain OUTPUT (policy ACCEPT) target prot opt source Chain POSTROUTING (policy ACCEPT)	destination
	target prot opt source	destination
	SNAT0.0.0.0/0 root@equipo02:/#	0.0.0.0/0 to:192.168.2.150
4	VMware Tools enables many features and improves mouse movement, vic performance. Log in to the guest operating system and dick Install Tools.	eo and Install Tools Remind Me Later Never Remind Me
To direct input to this VM	l, click inside or press Ctrl+G.	😗 🛶 🐂 ঝ 🖶 🛤 🗇 🗩 🖉

Comprobamos la Ip del equipo que está dentro de la red.



Comprobamos que el ordenador del exterior no puede conectar con el cliente de la lan.



Sin embargo el de dentro sí que puede conectar con el exterior.

Ubuntu_Desktop - VMware Workstation	- 0 <b>- X</b> -
File Edit View VM Team Windows Help	
Sidebar × 😰 ws2003 1 x 📸 Ubuntu Desktop x 🕼 Windows XP Proffesional 1 x 😰 Ubuntu Server X	
<ul> <li>▶ Powered On A Aplicaciones Lugares Sistema (2) (2)</li> <li>♥ Dismuty Desk</li> <li>♥ Undows XP</li> <li>♥ Fravites</li> <li>(2) Usuntu_Desk</li> </ul>	🛛 🚷 miguel 🕑 🕇 🛔
🙆 🛇 🔕 miguel@miguel: ~	
Archivo Editar Ver Terminal Ayuda	
miguel@miguel:-5 ping 192.168.2.151 Practica 1 Practica 1 Prac	
z I ge Conexiones de red	
To direct input to this VM, click inside or press Ctrl+G.	

## **CORTAFUEGOS:**

### 5. CORTAFUEGOS SOFTWARE.

- a) Cortafuego integrado en Windows. Instalación de software de cortafuegos en Windows y Linux:
- Instalar y configura el cortafuegos Kerio Winroute Firewall (Windows/Linux).

Nos descargamos la aplicación Kerio Winroute en nuestro equipo, que es un cortafuegos software muy potente para nuestro equipo (sólo entornos Windows.)



Comenzamos la instalación de la aplicación Kerio WinRoute.

Aceptamos los términos de licencia.



Marcamos las siguientes opciones para deshabilitar elementos como el firewall integrado de Windows y otros.



Introducimos el nombre de usuario y contraseña que usaremos para el administrador.



Comienza la instalación.



Una vez terminada la instalación finalizamos.



Ejecutamos la aplicación, y nos aparece esta ventana de autenticación.



Accedemos con la cuenta que nos hemos creado anteriormente.



La primera vez que accedamos nos aparecerá este asistente de configuración.



Elegimos la opción de único enlace de Internet.



Elegimos nuestra tarjeta o interfaz de red.

Windows XP Proffesional 1 - VMware Workstation	
File Edit View VM Team Windows Help	
Sidebar 🗙 🔄 ws2003_1 🗙 🛐 Windows XP Proffesional 1 🗙 📑 Ubuntu Server 🗙	
Powered On 🚱 localhost - Consola de administración para Kerio WinRoute Firewall	🔳 🖻 🔀
Parchivo Editar Ayuda	
B Sustarios y grupos	
🗟 🔛 Estado	<u> </u>
🗄 🔛 Registros	
Conexión persistente - página 3 de 7	
Selectione su interfaz de Internet:	
Directión IP: 10.33.2.145	
MAC: 00:0c:29:de:dd:33	uid 6399
Adaptador: AMD PCNET Family Ethernet Adapter (Microsoft's Pa	cket Scheduler)
	•
< <u>A</u> trás Siguie	ante > Cancelar 🗇 KERIO
Litte .	Varia WaBarta Sirawal 🔜 kashkatu44222 👂 ninyal 🏯 Lite
Listo Concella d	Neno walkouce mrewaal 🔄 localitosci 44333 🛛 🏹 Miguel 🔚 Lisco
To direct insuit to this VM click inside or more Ctdl G	

En esta pantalla, podemos escoger los protocolos a deshabilitar desmarcando el checkbox. Pero de momento, lo vamos a dejar como está.

🔲 Windows XP Proffesio	onal 1 - VMware Workstation		
File Edit View V	/M Team Windows Help		
🔲 💷 💽 🌍 🚺	🖄 🕼 🚺 🖬 🖬 🖬 💭 🔯		
Sidebar ×	🚳 ws2003_1 🗙 📑 Windows XP Pro	ffesional 1 🗙 🚰 Ubuntu Server 🗙	
Powered On	😡 localhost - Consola de administr	ción para Kerio WinRoute Firewall	_ 7 🗙
Favorites	Archivo Editar Ayuda		
🔂 Ubuntu_Desk	Kerio WinRoute Firewall	🔯 Kerio WinRoute Firewall	
	🗉 😋 coningaración 🗉 💕 Usuarios y grupos		
	🗄 🔛 Estado		
	🗉 🚉 Registros	😡 Asistente de reglas de red	
		Política saliente - página 4 de 7	
		Seleccione el nivel al que desea restringir el acceso a Internet de los usuarios de la LAN:	
		Permitir el acceso a todos los servicios (sin limitaciones)	
		Permitir el acceso sólo a los siguientes servicios:      Ild 6399	
		Servicio Protocolo Puerto de origen Puerto de destino D. Ali riginos reserveu.	
		HTTPS TCP Cualquiera 443	
		I SMTP TCP Cualquiera 21 P	
		DNS TCP/UDP Cualquiera 53     POP3 TCP Cualquiera 110	
		IMAP TCP Cualquiera 143     Indext TCD Cualquiera 22	
		< <u>Atrás</u> <u>Siguiente</u> > <u>Cancelar</u> <b>&amp; KERIO</b>	
	Listo.	📴 Kerjo WinRoute Firewall 💻 Incalhod: 44333 🔍 minuel	Listo
	🛃 Inicio 🛛 😂 🖻 🔼 🍘	oogle - Microsoft Int 😡 localhost - Consola d	<ul><li>5:07</li></ul>
To direct input to this VM	I, click inside or press Ctrl+G.		

Dejamos marcadas estas opciones.



Dejamos estas reglas por defecto.

📴 Windows XP Proffesional 1 - VMware Work	kstation	
File Edit View VM Team Window	ws Help	
🗕 II 🔽 🔄 🖄 🗊 🗔		
Sidebar × 🗗 ws2003_1 ×	🔐 Windows XP Proffesional 1 🗙 🖓 Libuntu Server 🛛 🗙	
🖃 🕨 Powered On 🛛 😥 localhost - Con	nsola de administración para Kerio WinRoute Firewall	
Windows XP Archivo Editar Ayud	da	
🔁 Ubuntu_Desk 😡 Kerio WinRoute	Firewall	
🗷 🖓 Configuració		
⊞ ≝ Estado	iupos ·	^
🗈 🔛 Registros		
	Sa Asistente de reglas de red	
	Politica entrante - pagina 6 de /	
	Si hay servidores ejecutándose en su LAN que quiera que estén disponibles desde Internet,	
	especinqueios a continuación. Si no, o no sade, saite esta pagina.	
	Firewall HTTPS wild 6300	
	Firewall Kerio VPN p. All rights reserved.	
		=
	Agregar Editar Quitar	
	<a>kERIO</a>	
Listo.	🔓 Kerio WinRoute Firewall 📃 localhost: 44333 🔱 miguel 🚝 Lis	to
- Inicio	🖸 🙆 🕂 🗿 Google - Microsoft Int 🔯 localhost - Consola d	5:08
To direct input to this VM, click inside or press	Ctrl+G.	

Por último finalizamos el asistente.

Uindows XP Proffesion	onal 1 - VMware Workstation		
File Edit View	/M Team Windows Help		
🔳 II 🕞 🧐 (	🛛 🕼 🗊 🗖 🗖 🕞 😨	) 🔤 🔄 🕼	
Sidebar ×	🙀 ws2003_1 🗙 🚮 Windows XP F	roffesional 1 🗙 👔 Ubuntu Server 🗙	
😑 🕨 Powered On	😡 localhost - Consola de adminis	tración para Kerio WinRoute Firewall 🛛 🦂	- 7 🗙
Windows XP	Archivo Editar Ayuda		
🔂 Ubuntu_Desk	🔛 Kerio WinRoute Firewall	Maria Min Dauta Firanall	
	🗷 🤤 Configuración		
	🗉 🥶 Osuanos y grupos		<u>^</u>
	🗄 🔂 Registros		
		🤬 Asistente de reglas de red 🛛 🔀	
		Finalizar - página 7 de 7	
		El Asistente ha recopilado toda la información necesaria y ahora generará las reglas. Si ha	
		facilitado información incorrecta o si su configuración de red cambia, debe ejecutar el	
		austerice de naeve para garana regias naevas	
		uid 6399	
		5. All high 5 reserved.	
		P C C C C C C C C C C C C C C C C C C C	
			=
			×
		Egi Kerio WinRoute Firewali 📃 localhost:44333 🔏 migu	el 🔁 Listo
۰		Google - Microsoft Int 🙀 localhost - Consola d	5:08
To direct input to this VM	l, click inside or press Ctrl+G.		🖥 🛤 🔲 💭 🔛 🖉

Nos situamos en política de tráfico. Donde podemos habilitar-deshabilitar diferentes protocolos de nuestro equipo.



Nos situamos en acceso a internet, y pulsamos a la casilla servicio. Se desplegará la siguiente ventana, donde podemos deshabilitar protocolos como en éste caso el HTTP.



Comprobamos al acceso a internet a través de otro protocolo, donde el resultado será:



Comprobamos una página con protocolo HTTPS, para comprobar que a éstas sí que podemos acceder.



Windows XP Proffesion	nal 1 - VMware Workstation							. C X
File Edit View VM	M Team Windows Help							
🔲 II 🕞 🌍 🚺	3 🕼 🕼 🛛 🗖 🗖 🗖 🕼 🕅	ai 📧 🛛 🚯						
Sidebar ×	🖓 ws2003_1 🗙 📸 Windows XP Pro	ffesional 1 🗙 🗗 Ubuntu Serve	r X					
😑 🕨 Powered On	🕼 localhost - Consola de administra	ación para Kerio WinRoute Fir	ewall					- 8 >
👘 Windows XP	Archivo Ayuda							
🖶 🥌 Pavontes	🐼 Kerio WinRoute Firewall							
	🖶 🏹 Configuración	🐌 Política de l	ráfico					
	Interfaces							
	Bandwidth Limiter	Nombre	Origen	Destino	Servicio	Acción	Regi: Traducción	
	Fitrado de contenido	Servicio HTTPS 😕	💠 Cualquiera	😥 Firewall	🖏 HTTPS	$\checkmark$		
	Servidor DHCP	Servicio Kerio VPN 😕	💠 Cualquiera	📁 Firewall	🔕 Kerio VPN	<b>√</b>		
	- 📩 DNS	🗹 Acceso a Internet (NAT) 📁	🚎 Fiables/locales	Internet	🖏 DNS	$\checkmark$	NAT	
	Our Definiciones	😡 Edita	r servicia/auerta		S FTP			
	Accounting				A HTTP			
	Opciones avanzadas	S DNS		Agregar 🔻	🖏 IMAP			
	🖲 😂 Usuarios y grupos	4 HTTE	5	Editar	S POP3			
	🖲 🔛 Estado	S IMAF	•	Outer	🖏 Telnet			
	🖻 🌄 Registros	Tráfico local	3		🔹 Cualquiera	1		
		<ul> <li>Teln</li> </ul>	et	Cualquiera		· 1		
				Borrar				
					*			
		M Tráfico del firew			CONS	<ul> <li>Image: A start of the start of</li></ul>		
					K HTTPS			
			Aceptar	Cancelar	🤹 IMAP			
					SMTP			
					🐝 Telnet			
		Bloquear otro tráfico 📁	💠 Cualquiera	💠 Cualquiera	🚸 Cualquiera	x		
			۲					
		Agregar Quitar					Asistent	.e
							Aplicar	Re <u>s</u> tablecer
-			🔓 Kerin WinRoute Firewa	l / Configuración / Política da tr	áfico 📃 localt	ost:44333	🤉 minuel 🛛 👼	Listo
		without Concelled A Report	to Particulares	wy coninguration y Policita de tr	unio 🖂 illali	030.77033		<b>1010</b>
< >		canost - Consola d	comandiculares			_		
To direct input to this VM,	click inside or press Ctrl+G.					-	) 🕑 🖼 📢 🚽 🛙	

Si de la misma manera, deshabilitamos el protocolo FTP.

Comprobamos que no podemos establecer conexiones FTP a través de internet.

Windows XP Proffesional 1 - VMware Workstation	Andrea Mil					- • X
File Edit View VM Team Windows Help						
- "	2 🔄 🕺 🚳					
Sidebar × 🗗 ws2003_1 × 🖓 Windows XP Prof	fesional 1 🗙 🚦 Ubuntu Server 🛛 🗙					
Powered On Windows XP Windows XP	ción para Kerio WinRoute Firewall					_ @ ×
Favorites						
🔁 Ubuntu_Desk 🧏 Kerio WinRoute Firewall	Política de tráfico					
- Interfaces						
😳 Polític	a fto			Acción	Regis Traducción	
Simbou det sister	nu - rep			1		
Servic ftp> open ftp.red	Settings>ftp liris.es		VPN	1		
DNS <pre>Ftp: connect :M</pre>	lúmero de error desconocido			1	NAT	
😥 💷 Defini				1		
			5			
- A Opcio						
B C Registro			t			
			uiera	<ul> <li>Image: A second s</li></ul>		
	7					Ŧ
			-	1		
			S HTTPS			
			Imap B POP3			
			SMTP			
		A	🗞 Teinet			
	Bloquear otro tráfico 🦻 💠 Cualquiera	💠 Cualquiera	💠 Cualquiera	*		
	Agregar Quicar				Asiste	ince
					Aglicar	Restablecer
	Eg Kerio WinRoute Firewal	l / Configuración / Política de trá	fico 🛛 🔜 local	host:44333	3 🙎 miguel 🚦	🗎 Listo
🐘 , 🥙 Inicio 🛛 😂 🗹 🗔 😡	alhost - Consola d 🚳 Banesto Particulares 🙉 Sint	iolo del sistema - ftp			(	5:19
a direct input to this VM, click inside or press Ctrl+G.				6	ə 💿 🐚 🗞 🖶	

En la opción interfaces, podemos seleccionar la interfaz que queramos. O configurar VPN.



Aquí podemos controlar el ancho de bando, haciendo diferentes limitaciones.



Aquí podemos realizar configuraciones, que por defecto ya realizan por defecto en el protocolo HTTP.



Hacemos configuraciones del DHCP.



Configuramos opciones de DNS.



Podemos comprobar la tabla de enrutamiento en esta ventana.



En opciones avanzadas, podemos realizar configuraciones más específicas del servicio.



Aquí podemos agregar y configurar usuarios, además de crear respectivos grupos.



📴 Windows XP Proffesio	onal 1 - VMware Workstation			and the second second		
File Edit View \	/M Team Windows Help					
	🗿 🕼 🗊 🗖 🗖 💭 🔯 I	M 🔄 🚯 🔊				
Sidebar ×	🗿 ws2003_1 🗙 📑 Windows XP Pro	offesional 1 🗙 🚡 Ubuntu Server	×			
Powered On	🚱 locathost - Consola de administración para Kerio WinRoute Firewall					
Favorites	Archivo Ayuda					
🔂 Ubuntu_Desk	🥵 Kerio WinRoute Firewall	Kerio WinRoute Firewall				
	Configuración     Interfaces		3			
	- 🐌 Política de tráfico - 🚱 Bandwidth Limiter		<u></u>			
		Firewall	Ayano RX	[KB/s] actual   1 × [KB/s] actual		
	Gilling HTTP					
	Política FTP					
	- 🔀 Antivirus	<b>*</b>				
	👺 Servidor DHCP	Información de host		Información de tráfico		
	A DNS     DNS     Definitiones	Host:	Firewall	Descargar:	475.16 KB (actual: 0 B/s)	
	- 🛵 Tabla de enrutamiento	Tiempo inactivo:	00:06:10	Cargar:	78.04 KB (actual: 0 B/s)	
	- 💫 Accounting	Tiempo de actividad 🔺	Evento de actividad	Descripción de actividad		
	- A Opciones avanzadas	05:11:39	WWW	Google MARCA.com		
	- & Usuarios					
	🖧 Grupos					
	🖃 🔛 Estado					
	Conexiones					
	🖐 Estadísticas					
	- 🕍 Clientes VPN					
	Mensajes de alerta					
		General Conexiones Hist	ograma			
					Ocultar detalles Actualizar	
			l Parazara are	en antiera de la caracteria de la composición de la composición de la composición de la composición de la compo	allast store   🔍 atsult 📑 the	
	Eg Kerio WinRoute Frewall / Estado / Hosts activos   🔤 locahost: 44333   👌 miguel   🤤 Listo					
Ta disast in such ta dh'i 100		ocanost * consula d	- Handedial 65			
To allect input to this viv	, circk inside of press curr+o.					

Aquí podemos auditar, los hosts a los que se ha accedido.

En esta pantalla, podemos auditar las conexiones realizadas entre el exterior y la propia red.



Image: View View View View View View View View	Windows XP Proffesio	al 1 - VMware Workstation					
Statur       Statures Str Professional 1       Statures str         Province       Statures Str Province       Statures Str Province         Province       Professional 1       Statures Str Province         Province       Province       Statures Str Province       Statures Str Province         Province       Province Str       Province Str Province       Province Str Province       Province Str Province         Province       Province Str Province         Province Str Province       Provin							
Powerd OR Windows XI Windows XI Wind	Sidebar X						
Windows X	Powered On	Inclusts Consult of Mindows Ar Professional Table Consultation Consult					
Fordets	🚯 Windows XP	Archive Ayuda					
Configuration Confi	Favorites	Rerio WinRoute Firewall					
	( <sup>2</sup> ) Ubuntu_Desk	<ul> <li>Concisioner averages de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión 6.3.0, Keric WirRoute Firewall de la versión 6.3.0, Keric WirRoute Firewall d'rince Estadísticas de la versión de la rea local - intervalos 20 segundos, tráfico desde 05/03/2012 5:01:41 (GHT+1:00)</li> <li>Forcessamiento Mirroute Firewall d'rince Estadísticas VIR Mirroute Firewall d'rince Estadísticas de uson for the versión de la versión de la versión de la v</li></ul>					
Histograma Ocultar detalles Cocultar detalles Co							
Histograma         Ocultar detalles         Actualizar           Cultar detalles         Actualizar         Eg. Kerio WinRoute Firewall / Estado / Estadisticas         Eg. Icalhost:+14333         A miguel         Eg. Listo		5					
🖁 🖁 Kerio WinRoute Firewall / Estado / Estadisticas 📃 localhost: 44333 🕹 miguel 👼 Listo		Histograma Ocultar getalles) Actuality	zar				
La Kolio Willicodo i Iloviali y Escado		📴 Kain Witting Example (Estado) (Estad					
Hicio 2 C I Clockhot - Consola d 3 Cuentas / Nómina - M		te Kello wirkoue mewai / Estabolicis 🔤 incanos:	5:28				
	To direct input to this VM						

Podemos observar un pequeño gráfico con las estadísticas de procesamiento.

En los registros, el administrador de red, puede consultar diversos informes acerca de diferentes campos, a los que el firewall está controlando.



## ii) Elabora un pequeño documento sobre Microsoft ForeFront y su funcionalidad en la empresa:

#### Microsoft Forefront: ¿Qué es Microsoft Forefront?

Microsoft Forefront es una completa línea de productos de seguridad que permite una mayor protección y control por medio de una excelente integración con su infraestructura de TI actual y una operación más sencilla de implantación, gestión y análisis. La línea de productos de seguridad Microsoft Forefront ofrece protección para las máquinas cliente, aplicaciones de servidor y la red perimetral.

Su completo conjunto de productos de seguridad, que se integran entre sí y con la infraestructura informática de su empresa, puede complementarse e interoperar con soluciones de terceros.

#### Una completa familia de productos

Microsoft Forefront ofrece una familia de productos de seguridad completa e integrada, que brindan protección para cliente, servidor y perímetro, de modo que su empresa esté a salvo de las amenazas que constantemente van evolucionando:

• Microsoft Forefront Client Security (anteriormente denominada Microsoft Client Protection).

• Microsoft Forefront Server for Exchange Server (anteriormente denominada Microsoft Antigen for Exchange).

• Microsoft Forefront Server for SharePoint<sup>®</sup> (anteriormente denominada Microsoft Antigen for SharePoint).

• Microsoft Forefront Security for Office Communications Server (anteriormente denominada Antigen for Instant Messaging).

• Microsoft Internet Security and Acceleration (ISA) Server 2006 (Descargue la información de este producto en XPS / PDF)

• Intelligent Application Gateway (IAG) 2007 (Descargue la información de este producto en XPS / PDF)

• Forefront Server Security Management Console.

#### Funcionalidades y ventajas

Todos ellos ofrecen una serie de funcionalidades y ventajas sobre los productos actuales de la competencia que podemos resumir en:

#### Protección para sistemas operativos

Forefront ayuda a proteger los sistemas operativos de clientes y servidores. Ofrece detección en tiempo real, programado o a demanda así como eliminación de virus, spyware, rootkits y otras amenazas emergentes.

#### Protección de aplicaciones de servidores críticas
Forefront ayuda a proteger los servidores de aplicaciones Microsoft a través de una estrategia de defensa en profundidad. ISA 2006 ofrece un sólido control de acceso e inspección de datos específicos de protocolo y de aplicaciones.

## Acceso seguro y controlado

Forefront ofrece una amplia gama de tecnologías de firewall, VPN y encriptación, así como funcionalidades de administración de identidades que ayudan a asegurar que sólo los usuarios autorizados tengan acceso a los datos y recursos de TI especificados.

## Protección de datos confidenciales

Los productos Forefront resguardan los datos confidenciales y protegen la propiedad intelectual. ISA 2006 proporciona una combinación de filtros específicos para cada aplicación en toda la red, como también tecnologías que garantizan la confidencialidad y autenticidad de los datos valiosos para su empresa.

## Integración desde el diseño

Los productos Forefront ofrecen múltiples niveles de integración, de modo que se pueda lograr una mayor eficiencia y control en términos de seguridad de la red.

## Integración con aplicaciones

Los productos anti-malware y de seguridad de acceso Microsoft Forefront están especialmente diseñados para proteger e integrarse con aplicaciones de servidores de misión crítica tales como Exchange, Outlook<sup>®</sup> Web Access y SharePoint.

## Integración con la infraestructura informática

Esta infraestructura unificadora permite administrar sin inconvenientes la implementación, distribución, configuración y aplicación de los productos de seguridad, y permite hacerlo con un nivel de control detallado y minucioso.

## Integración en Forefront

Los productos Forefront están diseñados para poder operar juntos, de modo que se puedan aprovechar sus funcionalidades y lograr una mayor cobertura de seguridad.

## Administración simplificada y centralizada

Los productos Microsoft Forefront están diseñados de forma tal que permiten simplificar la implementación, configuración, administración, generación de informes y análisis. De esta forma, su empresa tiene mayor confiabilidad en cuanto a una excelente protección.

### Implementación simplificada

Los utilitarios como ISA Server Best Practices Analyzer Tool y los asistentes de configuración ayudan a establecer una base sólida para una instalación de seguridad contundente. La integración de Forefront con Active Directory y los sistemas de actualizaciones como Systems Management Server proporcionan los cimientos comunes para la administración de configuraciones y cambios. Tanto los usuarios como los administradores se benefician con la distribución centralizada de

configuraciones y políticas actualizadas así como de actualizaciones de sistemas operativos o antivirus para clientes y servidores.

## Unificación de generación de informes y análisis

Forefront centraliza la recopilación y el análisis de la información de administración de seguridad, dado que toda la información de seguridad se almacena en un único repositorio SQL Server™, que puede utilizar los servicios de generación de informes y análisis (SQL Server Reporting and Análisis Services) para identificar e interpretar los eventos de seguridad.

## Administración simplificada

La administración y la generación de informes de seguridad están centralizadas en Forefront. Sus componentes se integran plenamente con los sistemas de administración existentes, incluyendo Microsoft Operations Manager, Microsoft Systems Management Server y Windows Server<sup>™</sup> Update Services. Las consolas de administración integradas de Forefront ofrecen las conocidas interfaces de Microsoft y son, además, fáciles de utilizar; por otra parte, reducen el tiempo de capacitación necesaria y ayudan a controlar los costes.

## Énfasis en la capacidad de "aseguramiento"

Al concentrar gran parte de sus esfuerzos en los aspectos relacionados con la integración y la administración de la seguridad –el "aseguramiento" de la infraestructura-, Forefront ayuda a su empresa a:

- Centralizar la administración de la seguridad.
- Evitar los errores en la configuración.
- Implementar la seguridad en toda la red.
- Obtener una visión unificada de la seguridad de la red.

## Conclusión

En conclusión, nos encontramos ante una familia de productos que, tanto juntos como de manera independiente, nos ofrecen una solución:

## Completa

A medida que los ataques aumentan, se tornan cada vez más costosos para su empresa, aumentando el tiempo de reposo necesario, la recuperación e impactando en forma negativa en la productividad y en la utilización de su software.

## Integrada

En general, los productos de seguridad no se integran mucho entre sí ni con la infraestructura de TI existente de uno. Esta falta de sinergia en la infraestructura actual hace que sea más difícil de controlar, creando potencialmente brechas e ineficiencias en la seguridad de su red.

Microsoft Forefront integra capacidades de seguridad en toda la línea de productos, con aplicaciones de servidor Microsoft y con su infraestructura de TI existente, de modo que usted puede lograr mayor eficiencia y control sobre la seguridad de su red.

## Simplificada

Puede ser difícil obtener visibilidad crítica acerca del estado de seguridad de su red, especialmente sin una herramienta de administración central. Sin este tipo de visibilidad, implementar y administrar la seguridad es más difícil, ineficiente, propicia al error y consume más tiempo.

Microsoft Forefront mejora su capacidad para mantener la seguridad de su organización al simplificar la administración, instalación y uso de los productos de seguridad, con lo que aumentará su confianza en que su organización está bien protegida.

Forefront aumenta la visibilidad en el estado de seguridad de su red al brindar una vista individual de la red, permitiendo una administración y una mitigación de amenazas mejor y más informadas.

http://www.microsoft.com/business/es-es/content/paginas/article.aspx?cbcid=225

- b) Distribuciones libres para implementar cortafuegos en máquinas dedicadas.
- i) Instalación y configuración del cortafuegos "Firewall Zentyal".

Tenemos el cortafuegos instalado por defecto en nuestro sistema, si nos situamos en cortafuegos, podemos configurar los siguientes escenarios.



## O en cambio éstos otros.

Zentyal - VMware Wo	orkstation	
File Edit View V	/M Team Windows Help	
🗖 🖬 💽 🧐 🚺	🖄 🕼 🔝 🚍 🕞 💭 🔤 🕵 🔇	
Sidebar ×	🚰 ws2003_1 🗙 🛐 Windows XP Proffesional 1 🗙 🛃 Ubuntu Server	× 🔐 Zentyal ×
Powered On     Windows XP	Nentyal -	Packet Filter - Mozilla Firefox _ © ×
👘 Zentyal	<u>File Edit View History Bookmarks Tools Help</u>	
B Vbuntu_Desk	😒 💿 👻 🔇 🕃 🛧 🚺 🚺 Iocalhost https://iocalhost/F	irewall/Filter 😭 🗸 Google 🔍
	Most Visited V Ozentyal.com Ozentyal.org ODocume	ntation OFrorum OOnline Store
	DNS 🗸	seguridad de su red, permittendo el acceso desde redes no conflables. Por favor, hágalo sólo si sabe lo que está haciendo.
	Servidor Web	Configurar reglas
	FTP	
	Autoridad de certificación	Reglas de filtrado desde las redes externas a las internas
	Office	Estas reglas le permiten controlar el acceso desde redes externas a redes internas
	Usuarios y Grupos	Debe saber que añadiendo reglas a esta sección puede estar comprometiendo la     seguridad de su red, permitiendo el acceso desde redes no confishes. Per favor, bánalo
		sólo si sabe lo que está haciendo.
	Webmail	Configurar reglas
	ઉ€₫℃∞	Reglas de filtrado para el tráfico saliente de Zentyal Estas reglas permiten controlar el acceso desde Zentyal a servicios externos. Configurar reglas
		Reglas añadidas por servicios de Zentyal (Avanzado)
		Estas reglas son automáticamente agregadas por los servicios de Zentyal.
		Puede deshabilitar estas regias, pero debe estar seguro de lo que está haciendo o algunos servicios podrían detenerse.
		Configurar reglas
	Zentyal	created by eBox Technologies S.L.
		12:24 🗐 🚺
< III > To direct input to this VM	= · · · · · · · · · · · · · · · · · ·	
Les ances input to this the	,	

Escogemos la primera opción, ya que vamos a denegar un servicio a un PC de nuestra LAN para comprobar el resultado de nuestro cortafuegos.

Zentyal - VMware Workstation	A Response to the second		the lot of the lot of the lot of the							
File Edit View VM Team Windows	Help									
	i 🖸 🕞   🖾 🖾 🔝   🖧 🚯									
idebar × ws2003_1 ×	Windows XP Proffesional 1 🗙 🚡	Ubuntu Server 🗙 🛅 Ze	ntyal 🗙							
Windows XP	ی می Zentyal Mozilla Firefox ـ ۵ ×									
Zentyal <u>File Edit V</u> iew	<u>Eile Edit View History Bookmarks Tools H</u> elp									
Favorites	) 💿 🛧 🚺 localhost http	os://localhost/Firewall/Vi	ew/InternalToEBoxRuleTable	r 🗸 🖌	Google					
🖞 Ubuntu_Desk 📷 Most Visited 🗸	Ozentyal.com Ozentyal.or	g 🔿 Documentation 🌾	>Forum Online Store							
🔿 zent	Cerrar sesión	Guardar cambios								
	Filtrado de paqu	<u>ietes</u> ► Desde rede	s internas hacia Zentyal							
Core	Añadiendo un/a r	uevo/a regla								
Dashboard	Decisión: DENEGAR	\$								
Estado de los Mo	odulos Origen: IP Origen	0 10.33.2.120	/ 32 0							
Sistema	Servicio:	Servicio:								
Red	Si la selección inversa está marcada, la regla será aplicada cualquier servicio excepto el seleccionado									
Mantenimiento	Descripción: 2003 Server									
Gestion de sortw	are									
Gateway	Gateway Proxy HTTP Desde redes internas hacia Zentyal									
Proxy HTTP										
UTM		Buscar								
Filtrado de page	Decisión	Origen	Servicio	Descripción	Acción					
Redirecciones o	ie 🔨	Cualquiera	FTP		窗 🖉 🗸					
VPN	<b>^</b>	Cualquiera	dns	-	<b>宙 ∠ ↑ ↓</b>					
Infrastructure	<b>^</b>	Cualquiera	http		窗 🖉 🛧 🗸					
DHCP	<b>^</b>	Cualquiera	Mail Submission		亩∠↑↓					
DNS	DNS Cualquiera Incoming Mail									
FTP	<b>^</b>	Cualquiera	SMTP		11 L A					
https://localhost/	Firewall/View/InternalToEBoxBul	eTable#								
	Zentval Mozilla Firefox	root@equipo02: /ho	me/		13:16 💷					
	4.6	1.22								

Una vez configurado guardamos los cambios. Hemos denegado el protocolo ICMP para el equipo 10.33.2.120.

Zentyal - VMware Wo	orkstation		8 - Thurs	March March Street	-					
File Edit View V	/M Team Windows Help									
Zertyd - VMaew Workstation       Image: Sector										
Sidebar ×	🔐 ws2003_1 🗙 🐴 Windows XF	Proffesional 1 🗙	🔋 Ubuntu Server 🛛 🗙 🎦 Zentya	I X						
Windows XP	0		Zentyal Moz	illa Firefox			- 0 ×			
Zentyal	Eile Edit View Higtory Bookmarks Tools Help									
□ ♥ Favorites	😋 🔘 v 🔇 😂 <u>(</u>	🚡 🚺 localhost ht	tps://localhost/Firewall/View/I	nternalToEBoxRuleTable	☆ ✔ 🛃 ¥	Google	0			
🖆 Ubuntu_Desk	Most Visited ✓ Ozenty	/al.com 🔿 zentyal.c	org ODocumentation OFo	orum 🜔 Online Store						
sidedit <pre></pre>										
	Dashboard	Filtrado de paq	<u>uetes</u> ► Desde redes in	ternas hacia Zentyal						
Sidesr       Image: Sidesr										
	Bar									
	Red		Buscar	Zentyal X  Zentyal X  Mozilla Firefox  Mozilla Firefox  Mozilla Firefox  Mozilla Firefox  Mozilla Firefox  Mozilla Firefox  Cerrar sesión  Courdar cambios  Cerrar sesión  Courdar cambios  des internas hacia Zentyal   Servicio  Prip  KMP  Courdar cambios  Cerrar sesión  Courdar cambios  des internas hacia Zentyal  Cerrar sesión  Courdar cambios  Cerrar sesión  Cerrar sesión  Courdar cambios  Cerrar sesión  Cerrar sesión  Courdar cambios  Cerrar sesión  Cerrar sesión  Courdar cambios  Cerrar sesión  Courdar cambios  Cerrar sesión  Cerrar sesión  Cerrar sesión  Cerrar sesión  Cerrar sesión  Cerrar ses						
	Mantenimiento	Decisión	Origen	Servicio	Descripción	Acción	=			
	Suscripción	×	10.33.2.120/32	ICMP	2003 Server	亩 🖉 🗸				
	Gateway	•	Cualquiera	FTP		<b>₩</b>				
	Proxy HTTP	<b>^</b>	Cualquiera	dns		** ∕ ↑ ↓				
	Cortafuegos	1	Cualquiera	http		亩∠↑↓				
	Filtrado de paquetes	•	Cualquiera	Mail Submission		╈╱办Ψ				
	Redirecciones de puertos	<b>^</b>	Cualquiera	Incoming Mail		亩∠↑↓				
	VPN	<b>^</b>	Cualquiera	SMTP		₩ 🖉 🛧				
	Infrastructure				10 2 Página					
	DNS				C- O rugin					
	Servidor Web			Server × 2 Zentyal ×         Zentyal - Mozilla Firefox         calhost/Firewall/View/InternalToEBoxRuleTable         icalhost/Firewall/View/InternalToEBoxRuleTable         icalhost/Firewall/View/InternalToEBoxR						
Proveed On Windows XM Proveed On			~							
	https://localhost/Firewall/Vi	ew/InternalToEBoxR	uleTable#			13:16				
• <u> </u>	🔚 🖓 💙 😎 📣 🞯 Zen	tyai Mozilla Hrefox	root@equipo02: /nome/			13.16				
to airect input to this VM	, click inside or press Ctri+G.				🔁 🖨 🖯	🛯 🐝 🖼 💷 💭 💭				

Comprobamos nuestra IP de Zentyal.



Comprobamos la IP del cliente denegado, y comprobamos que no puede conectar con el Zentyal, por el cortafuegos.



Sin embargo, a la inversa sí que podemos.

Edit View VM	Team Windows Heln										
Powered On	👔 ws2003_1 X 🛐 Windows XP Proffesional 1 X 📑 Libuntu Server X 📅 Zentyal X										
Windows XP	Zentyal Mozilia Firetox - 5  Eila Edit View History Rockmarks Table Help										
Zentyal	Elle Fair Alem Histola Rookuyauka Toola Helb										
Favorites	🗦 😳 🖌 🔇 😣 🕻	localhost h	ttps://localhost/Firewall/View/	InternalToEBoxRuleTable	☆ ✔ 🛃 ٧	Google					
😰 Ubuntu_Desk 📘	Most Visited 🗸 🔿 zenty	al.com 🔿 zentyal.	org ODocumentation OF	orum 🜔 Online Store							
	zentyai					Guardar cambios					
	-	Filtrado de par	ulatas - Desde redac in	ternas bacia Zentual							
	<u>_</u>	i indauo ue pat	ueres > Desue redes In	itemas nacia Zentyal							
	Dashboard	Configure Rules	5								
		Añadir nuevo/a									
'	Estado de los Modulos		Buscar								
1	Sistema										
	Red	Decision	Origen	Servicio	Descripción	Accion					
	Mantenimiento	×	10.33.2.120/32	ICMP	2003 Server	窗 🖉 🗸					
	Sestión de software	Υ.	Cualquiera	FTP		亩 🖉 🛧 🗸					
1	Suscripción	<b>^</b>	Cualquiera	dns		<b>亩</b> ∠↑↓					
-	ateway	•	Cualquiera	http		亩∠↑↓					
	тм	•	Cualquiera	Mail Submission		亩 / <b>小</b> 山					
	Cortafuegos		cauquera	Han Sabinisation							
	Filtrado de paquetes		Cualquiera	root@equipo02: /home/mi	guel						
	Redirecciones de puertos	Archivo	<u>E</u> dición <u>P</u> estañas Ay <u>ı</u>	<u>i</u> da							
	/PN	root@equ	ipo02:/home/miguel#	ping 10.33.2.120							
	nfrastructure	PING 10.	33.2.120 (10.33.2.1	20) 56(84) bytes of	data.						
	DHCP	64 bytes	from 10.33.2.120:	icmp_seq=1 ttl=128 t	ime=17.7 ms						
I	DNS	64 bytes	from 10.33.2.120:	<pre>icmp_seq=2 ttl=128 t</pre>	ime=0.585 ms						
	Servidor Web	°C by tes	110m 10.33.2.120:	icmp_seq=3 ttt=128 t	1me=0.487 MS						
				ticc							
2	TP	10.3	3.2.120 ping statis	LICS ····							
1	-TP	10.3 3 packet	3.2.120 ping statis s transmitted, <u>3 re</u>	ceived, 0% pack <u>et lo</u>	ss, time 2001ms	5					

ii) Instalación y configuración del cortafuegos "Firewall IpCop".

Introducimos la ISO de la aplicación, y arrancamos la máquina virtual, una vez arrancado, procedemos a instalarlo en nuestro idioma.



Confirmamos el siguiente mensaje.



Elegimos instarlo desde la primera opción.



Nos indica el disco donde se llevara a cabo la instalación, que en este caso es /dev/sda



Nos saltamos el proceso de backup.



Comprobamos nuestras tarjetas, con la opción prueba.



Una vez nos detecte las tarjetas de red, aceptamos.



Elegimos la primera interfaz, que será **green**, y configuramos la direcciones IP de la siguiente manera.



- - X IPCop - VMware Workstation File Edit View VM Team Windows Help 🗖 💷 🕞 🔄 🔯 🎊 🎲 🗐 🖬 🔂 🕞 🐨 🔤 🔄 1 🔁 🚯 × 🛐 ws2003\_1 🗙 🗗 Windows XP Proffesional 1 🗙 📑 Ubuntu Server Sidebar 🗙 🚰 Zentyal 🗙 👘 IPCop 🗙 😑 👂 Powered On IPCop v1.4.20 - The Bad Packets Stop Here 👘 ІРСор 🖃 🤍 Favorites Felicitaciones! 🖆 Ubuntu\_Desk 👘 ІРСор IPCop ha sido instalado exitosamente. Por favor, quite el disquete o CD que pueda tener en su PC. Se iniciará el Setup, en el podrá configurar ISDN, tarjetas de red, y contraseñas del sistema. Luego de finalizado el Setup, podrá apuntar su navegador web a http://ipcop:81 o https://ipcop:445 (o como nombró su IPCop), y configurar los accesos telefónicos y/o los accesos remotos que correspondan a su instalación. No olvide adjudicar una contraseña para el usuario "dial" en su IPCop, si no desea que usuarios "admin" puedan controlar el enlace. OK Install MS-DOS as you would on a physical computer. Click in the virtual screen When you are done and the operating system boots up, click I Finished Installing. Change Disc Help to send keystrokes .... - F To direct input to this VM, click inside or press Ctrl+G. 💿 🛶 💾 🖫 🍫 🛛 📰

Una vez las tengamos pulsamos OK.

Elegimos nuestro mapa de teclado, que es en nuestro caso es.



Elegimos nuestra zona horaria, Europe/Madrid



Introducimos el nombre de la máquina, ipcopmiguel

IPCop - VMware Workstation
File Edit View VM Team Windows Help
Sidebar 🗙 🗗 ws2003_1 🗙 🗗 Windows XP Proffesional 1 🗙 🗗 Ubuntu Server 🗙 🗗 Zentyal 🗙 🚮 IPCop 🗙
□ Powered On IPCop v1.4.20 - The Bad Packets Stop Here
🕞 PCop
🔁 Ubuntu_Desk
Nombre de ordenador
Ingrese el nombre de host para su máquina.
inconniquel
OK Cancelar
<tab>/<alt-tab> entre elementos   <space> para_seleccionar</space></alt-tab></tab>
Citatis the visitual excess I Install MS-DOS as you would on a physical computer.
Unce in the virtual screen when you are done and the operating system boots I Finished Installing Change Disc Help up, click I Finished Installing.
To direct input to this VM, click inside or press Ctrl+G.

Ingresamos el nombre de nuestro dominio, miguelasir.



Inhabilitamos la configuración de RDSI.



Una vez realizados los pasos anteriores, accedemos a este menú de configuración, que configuramos uno a uno.



Elegimos el tipo de configuración **GREEN + RED**, que corresponden a nuestras 2 tarjetas de red instaladas en la máquina.



- -IPCop - VMware Workstation File Edit View VM Team Windows Help = II 🔊 🧐 🔯 🕼 🕼 🗐 🖬 🖬 🔄 🔛 🔝 i 🚺 🚯 🗙 📑 Windows XP Proffesional 1 Sidebar х 🔁 ws2003\_1 🗙 🖆 Ubuntu Server 🗙 🚰 Zentyal 🗙 📑 IPCop 🗙 IPCop v1.4.20 - The Bad Packets Stop Here 😑 👂 Powered On 🐴 IPCop 🖃 🤍 Favorites — Menu de configuración de red — 🛅 Ubuntu\_Desk 👘 IPCop Configuración actual: GREEN + RED La configuración ha sido completada, necesita reiniciar la red. Tipo de Configuración de Red. Controladores y tarjetas asignadas Configuración de direcciones Opciones de DNS y Gateway Configuración del servidor DHCP Acabado <Tab>/<Alt-Tab> entre elementos | <Space> para seleccionar Install MS-DOS as you would on a physical computer. When you are done and the operating system boots up, click I Finished Installing. Elick in the virtual screen to send keystrokes ш To direct input to this VM, click inside or press Ctrl+G. 💿 🛶 💾 🖏 🍫 📗

Pulsamos la opción controladores y tarjetas asignadas.

Pulsamos OK para habilitar la segunda tarjeta de red, RED.



Configuramos las direcciones de nuestra tarjeta.



Elegimos la interfaz **GREEN** o tarjeta número 1.

IPCop - VMware Work	kstation
File Edit View V	(M Team Windows Help
🗖 🔲 🚺 🗳 🚺	
Sidebar ×	🖆 ws2003_1 🗙 🗗 Windows XP Proffesional 1 🗙 🗗 Ubuntu Server 🗙 🗗 Zentyal 🗙 👘 IPCop 🗙
<ul> <li>Powered On</li> <li></li></ul>	IPCop v1.4.20 - The Bad Packets Stop Here
🔒 ІРСор	Configuración de direcciones
	Selecciona el interfaz que deseas volver a configurar
	CREEN RED
	OK Acabado
	$(T_{ab})/(Alt-T_{ab})$ entre elementos   (Snace) nara seleccionar
< +	Click in the virtual screen to send keystrokes Install MS-DOS as you would on a physical computer. When you are done and the operating system boots I I Finished Installing Change Disc Help
To direct input to this VM,	, click inside or press Ctrl+G. 💿 🖵 🖽 🍫 📔 📶

Establecemos las direcciones IP si no las tuviéramos, pero ya las hemos configurado anteriormente.



Elegimos la interfaz RED o tarjeta número 2.

IPCop - VMware Workstation	
File Edit View VM Team Windows	Help
🗖 🖬 🕟 🧐 🔯 🕼 🗊 🗖	
Sidebar × 🗗 ws2003_1 🗙	Windows XP Proffesional 1 🗙 🗗 Ubuntu Server 🗙 🗗 Zentyal 🗙 🔂 IPCop 🗙
<ul> <li>▷ Powered On</li> <li>☆ IPCop</li> <li>○ Favorites</li> <li>☆ Ubuntu Desk</li> </ul>	IPCop v1.4.20 - The Bad Packets Stop Here
🕞 ІРСор	Configuración de direcciones
s	elecciona el interfaz que deseas volver a configurar
	GREEN RED
	OK Acabado
(Ta	N/(Alt-Tab) entre elementos   (Space) para seleccionar
Click in the virtual so	een Install MS-DOS as you would on a physical computer. When you are done and the operating system boots up, dick I Finished Installing.  I Finished Installing Change Disc Help
To direct input to this VM, click inside or press Ctr	+G. 💿 🛶 💾 🖏 🦚 📄 🦼

Establecemos la dirección IP de esta interfaz.



Como ya hemos configurado las dos interfaces, acabamos el proceso.

IPCop - VMware Workstation	
File Edit View VM Team Windows Help	
Sidebar 🗙 🗗 ws2003_1 🗙 🗗 Windows XP Proffesional 1 🗙 🗗 Ubuntu Server 🗙 🗗 Zentyal 🗙 🔐 IPCop	×
□ ▷ Powered On IPCop v1.4.20 - The Bad Packets Stop Here ③ IPCop □ ♥ Favorites	
🔁 Ubuntu_Desk	
Configuración de direcciones	
Selecciona el interfaz que deseas volver a configurar	
GREEN	
OK Acabado	
<tab>/<alt-tab> entre elementos   <s<u>pace&gt; para seleccionar</s<u></alt-tab></tab>	·
Click in the virtual screen Unstall MS-DOS as you would on a physical computer, When you are done and the operating system boots Up, click I Finished Installing. Change Disc	Help
To direct input to this VM, click inside or press Ctrl+G. 💿 🕁 [	- 🗟 🗞 📄 /



Accedemos a las opciones de DNS y puerta de enlace.

Ingresamos la información de las DNS y la puerta de enlace a internet.



Por, último si queremos, hacemos la configuración del servidor DHCP, seguidamente pulsamos OK, y finalizamos la configuración.



Ingresamos la contraseña para el usuario root, que será "invesinves".





Ingresamos la contraseña para el administrador de IPCot.

Además ingresamos una contraseña para la realización de backups de forma segura.



Una vez configurado todo perfectamente, pulsamos OK en esta pantalla y reiniciamos la máquina.



Arrancamos el sistema, y apreciamos un arranque similar a otros sistemas Linux.



#### Nos logueamos como root.



Ejecutamos un **ipconfig** para comprobar que nos ha almacenado el valor de las tarjetas de red.



Desde un cliente, accedemos a la máquina vía web. Nos logueamos con la cuenta de administrador.



Podemos realizar diversas tareas con esta aplicación, como por ejemplo mirar el estado del sistema.



Podemos comprobar el estado de las interfaces de la máquina, que hemos configurado anteriormente.



Podemos habilitar el acceso ssh a la máquina.



Windows YP Proffesion	al 1 - VMware Worksta	tion				
File Edit View VM	A Team Windows	Help				
Sidebar ×		Windows VP Profferional 1	Ibunhi Sanjar 😵 🖪 Zanh			
🖃 🕨 Powered On	PCon - Configura	ción de acceso externo - Microso	nft Internet Explorer			
IPCop	Archivo Edición Ver	Eavoritos Herramientas Ayuda				
Favorites     Duntu Desk	😪 Atrás 🔹 🕥 -	💌 💈 🏠 🔎 Búsqueda	🛧 Favoritos 🕢 🔗 -	2 🕹		
🚯 IPCop 🛛	Dirección 🕘 https://192	.168.2.150:445/cgi-bin/xtaccess.cgi				💌 🄁 Ir Vínculos
] 1	FIREWAL SISTEMA	L 🚸 Acceso externi > Estado + Red +	SERVICIOS * FIREWALL *	The bad packets sto	p here.	
	Editar u	n regla existente:				
	(				R	
	TCP 💌	IP de origen, o red (vacio pa	ra "TODAS"): 0.0.0.0/	)	Puerto de la	destinación: 21
	Activo: 🗹	IP Destino: DEFAULT IP	•			
	Observaci	in: • FTP				
	• Este car	npo puede quedar vacio.			Actualizar	9
	Reglas a	ctuales:				
	Proto	IP de Origen	IP Destino	Puerto de la destinación	Observaci	ón Acción
	TCP	TODO	DEFAULT IP	113		☑ / ᠿ
	тср	TODO	DEFAULT IP	21	FTP	
Prove Charge Configuración do acceso externo - Microsofi Internet Explorer         Prove Charge Configuración do acceso externo - Microsofi Internet Explorer         Prove Charge Configuración do acceso externo - Microsofi Internet Explorer         Prove Charge Configuración do acceso externo - Microsofi Internet Explorer         Prove Charge Configuración do acceso externo - Microsofi Internet Explorer         Prove Edos yer yeveto Berametris - Ayda         Prove Charge Configuración do acceso externo - Microsofi Internet Explorer         Prove Edos yer yeveto Berametris - Ayda         Prove Charge Configuración do acceso externo - Microsofi Internet Explorer         Prove Edos yer yeveto Berametris - Ayda         Prove De Charge Configuración do acceso externo - Microsofi Internet Explorer         Prove De Charge Configuración do acceso externo - Microsofi Prove Configuración - Origina         Prove De Charge Configuración - Origina - Destino - De						
-	D D	<b>.</b> 2	00:37:	Conectado (O 54 up 3:03, 1 user, loar	<mark>d 3h 3m 6s)</mark> d average: 0.00, 0.00, 0.00	SOURCEFORGE.MET
	🛃 Listo					🔒 🥥 Internet
	🐉 Inicio 🔰 😂	🞯 📶 💊 Conexiones de red	🔤 Símbolo del sistema	🐴 IPCop - Configuraci	ó	2:03
o direct input to this VM, o	click inside or press Ctrl	+ G.				🛶 💿 🖏 🌒 🖷 🛤 📁  🔛

En acceso externo, deshabilitamos el servicio FTP por el puerto 21

También podemos denegar las respuestas de ping a las interfaces, aquí por ejemplo denegamos la tarjeta roja o 2º interfaz.



Comprobamos que podemos hacer ping con el cliente a la tarjeta verde, pero no a la roja.



Comprobamos también que no podemos acceder al servicio FTP.



Windows XP Proffesional	1 - VMware Workstation	0 · 3 8 8 4 mm	_ 0 ×
File Edit View VM	Team Windows Help		
🗖 II 🕅 🌚			
Sidebar ×	ws2003_1 × 🔐 Windows XP Proffesional 1 × 🔮 Ubuntu Server × 🖓 Zentyal × 🚯 IPCop ×		
Powered On	IPCop - Configuraciones del Control de Tráfico - Microsoft Internet Explorer		
Windows XP	rchivo Edición Ver Eavoritos Herramientas Ayuda		A.
⊨ ♥ Favorites ∯ Ubuntu_Desk	🔾 Atrás 🔹 😥 🕐 📓 🏠 🔎 Búsqueda 🤸 Favoritos 🤣 🎯 - 📚 🗔 🦓		
Dir Dir	regción 🧶 https://192.168.2.150:445/cgi-bin/shaping.cgi		Y 🔁 Ir Vínculos 🎽
1.4	SISTEMA + ESTADO + RED + SERVICIOS + FIREWALL + VPNS + LOGS	here.	
	Configuraciones:		
	Control de Tráfico		
	Velocidad de baiada (kbit/seg): 100		
	Velocidad de subida (kbit/seg):		
		Guardar	2
	Agregar servicio	2	
	Prioridad: Alta 💌 Puerto: Protocolo: TCP 💌	Activo:	
		Agregar	
	Opciones de Control de Tráfico	2	
	Prioridad Puerto	Protocolo	Acción
Ē			Internet
· <	🚺 INICIO 😕 🕼 🔼 💊 Conexiones de red 🔤 Símbolo del sistema - Îtp 🖉 IPCop - Configuracio.		2:08
To direct input to this VM, cli	ick inside or press Ctrl+ G.	G	) 🖫 📢 🖼 🛤 📁  🔝 🏼

Podemos realizar en control de tráfico un control del mismo.

Podemos configurar en servidor de horario un servidor NTP.

Windows XP Proffesio	onal 1 - VMware Workstation	x
File Edit View \	/M Team Windows Help	
🔳 II 🕞 😋 🛔		
Sidebar ×	🗿 Ivs2003_1 🗙 🗃 Windows XP Proffesional 1 🗙 🗿 Ubuntu Server 🗙 🚳 Zentyal 🗙 👘 IPCop 🗙	
Powered On	🖻 IPCop - Configuración NTP - Microsoft Internet Explorer 💦 👘 🗐 🖻	×
Windows XP	Archivo Edición Ver Eavontos Herramientas Alyuda	ľ
Generation     Generation     Generation     Generation     Generation     Generation	🔇 Atris - 🕥 - 🖹 🖉 🏠 🔎 Büsqueda 👷 Favoritos 🤣 🍰 - 🌺 🔜 🦓	
тр ГРСор	Dirección 🕘 https://192.168.2.150.445/cg-bin/bine.cgi	; "
	SERVICIOS * SERVIDOR DE HORARIO · The bad packets stop here.	<u> </u>
	Usa un Network Time Server:	
	Obtener la hora desde un Servidor de Horarios para Redes (NTP)     El reloj no ha sido sincronizado     Servidor NTP primario:     Dipcop.pool.ntp.org     Servidor NTP Secundario:     1.ipcop.pool.ntp.org     Proporcionar el tiempo a la red local	
	Actualizar hora         Para solicitar una sincronización no programada, presione el botón Cambiar Hora Abora. Tenga en cuenta que debe esperar S minutos, o más, para que la sincronización se complete.         Cada:       1         I       dias	
	• Este campo puede quedar vacio. Cambiar Hora Ahora Guardar 🥹	
	Actualizar hora	
	Año: 2012 Mes: 03 Día: 06 Horas: 00 Minutos: 43 Actualización Instantánea	
		~
	Internet	
<	🚺 Inicio 🔰 🗵 🕼 🔽 🖒 Conexiones de red 🔤 Sixibolo del sistema - ftp 🔄 IPCop - Configuració 🔇 🕵 2.4	9
To direct input to this VM	1, click inside or press Ctrl+G. 📮 💬 🐯 🖓 👾 💷 🗇	1

También podemos destacar el estado de las conexiones, para auditar todas las conexiones con la máquina.

Windows XP Proffesio	onal 1 - VN	Aware Workstati	on					0.1080	C . C		×
File Edit View V	M Tean	n Windows	Help								_
	sa isa 11		9 🖌   🖾 I	s 🔝   😰 🗊	>						
Sidebar ×	🖆 ws200	03_1 × 🛅 V	Nindows XP Pro	ffesional 1 🛛 🕹 🚦	υ	buntu Server 🛛 🗙 🗿 Z	entyal 🗙 🐴 IPCop	×			
Powered On	🗿 IPCop	p - Conexiones	- Microsoft Ir	ternet Explorer							BX
Windows VD	Archivo	Edición <u>V</u> er	Eavoritos Herr	amientas Ay <u>u</u> da							
= Savorites	<b>A</b>		🗅 🖻 🥢								
Ubuntu_Desk	G Atr	as • 🕤 ·	📕 🖻 🚺	Busqueda	2	Favoritos 😸 🖂	i 🖉 🖉				
🐴 IPCop	Dirección	🕘 https://192.1	.68.2.150:445/cg	-bin/connections.cgi						🗸 🔁 Ir 🛛 Vi	nculos
		Estado						4200	19		
	Con	Latado		CUNEXIONES			The bad packets	stop here.			
	1.4.20	SISTEMA 4	ESTADO 4	RED 🔹	S	ERVICIOS * FIREWALI	. ∳)¥PNS ∳)L	ocs 🔹 🏹 🛃	e la		
				MARCADO	_						
	1	Rastreo de	Conexión de	CARGAR IF MODEM							
				ALTAS							
		Leyend	a: LAN	INTERNE	т	DMZ In	alambrica I	PCop VPN			
		Protocolo	Caducidad (Segundos)	Conexión Estado		Original IP:Puerto de Origen	Original IP:Puerto de destino	Esperado IP:Puerto de Origen	Esperado IP:Puerto de destino	Marcado	,
		Todos/as 💌		Todos/as	۷	*.*.*.* 💌	••••	Clase en Orden Asc	endente: orgsip 💌	Todos/as	~
		udp (17)	2			127.0.0.1 :32768	<u>127.0.0.1</u> :53	<u>127.0.0.1</u> :53	127.0.0.1 :32768	[UNREPLIED	DJK
		udp (17)	8			<u>127.0.0.1</u> :32770	<u>127.0.0.1</u> :53	<u>127.0.0.1</u> :53	<u>127.0.0.1</u> :32770	[UNREPLIED	D]
		udp (17)	5			<u>127.0.0.1</u> :32769	<u>127.0.0.1</u> :53	<u>127.0.0.1</u> :53	<u>127.0.0.1</u> :32769	[UNREPLIED	D]
		tcp (6)	103	TIME_WAIT		<u>192.168.2.145</u> :1139	<u>192.168.2.150</u> :445	<u>192.168.2.150</u> :445	<u>192.168.2.145</u> :1139	[ASSURED	21
		tcp (6)	85	TIME_WAIT		<u>192.168.2.145</u> :1136	<u>192.168.2.150</u> :445	<u>192.168.2.150</u> :445	<u>192.168.2.145</u> :1136	[ASSURED	2]
		top (6)	66	TIME_WAIT		192.166.2.145 (1131	192.168.2.150 :445	<u>192.168.2.150</u> :445	192.168.2.145 (1131	[ASSURED	21 51
		tcp (6)	73	TIME WAIT		192,168,2,145 :1133	192.168.2.150 :445	192,168,2,150 :445	192.168.2.145 :1133	[ASSURED	0 )]
		tcp (6)	431999	ESTABLISHED		192.168.2.145 :1140	192.168.2.150 :445	192.168.2.150 :445	192.168.2.145 :1140	[ASSURED	51
		tcp (6)	19	TIME_WAIT		192.168.2.145 :1129	<u>192.168.2.150</u> :445	<u>192.168.2.150</u> :445	<u>192.168.2.145</u> :1129	[ASSURED	5]
		tcp (6)	76	TIME_WAIT		<u>192.168.2.145</u> :1134	<u>192.168.2.150</u> :445	<u>192.168.2.150</u> :445	<u>192.168.2.145</u> :1134	[ASSURED	)]
		tcp (6)	71	TIME_WAIT		<u>192.168.2.145</u> :1132	<u>192.168.2.150</u> :445	<u>192.168.2.150</u> :445	<u>192.168.2.145</u> :1132	[ASSURED	2]
		tcp (6)	82	TIME_WAIT		<u>192.168.2.145</u> :1135	<u>192.168.2.150</u> :445	<u>192.168.2.150</u> :445	<u>192.168.2.145</u> :1135	[ASSURED	2]
		udp (17)	8			<u>192.168.2.150</u> :50337	<u>8.8.8.8</u> :53	<u>8.8.8.8</u> :53	192.168.2.150 :50337	[UNREPLIED	5]
		udp (17)	2			<u>192.168.2.150</u> :48885	8.8.8.8 :53	8.8.8.8 :53	<u>192.168.2.150</u> :48885	UNREPLIED	_]
		udp (17)	5			192,100,2,150 192,168,2,150,42189	8888.53	8888.53	192.100.2.150 :50337		-) -)
		udp (17)	2			192.168.2.150 :48885	80.58.61.254 :53	80.58.61.254 :53	192.168.2.150 :48885	UNREPLIE	D1
		udn (17)	5			192.168.2.150 :42189	80.58.61.254 :53	80.58.61.254 :53	192.168.2.150 :42189	[LINREPLTER	ח
	<										>
	e				_				🔒 🔮 Ir	nternet	
4 III +	🏼 🛃 Ini	icio 🦯 🥭	🥶 🗖 💊 o	onexiones de red		Símbolo del sistema -	ftp 🛛 🐴 IPCop - Conexi	ones		ં ્રેક્રેક	2:11
o direct input to this VM	l, click insid	de or press Ctrl+	G.						🛶 💿 🔩	📣 🖶 🛤 📁	

# 6. CORTAFUEGOS HARDWARE.

# a) Elabora un informe sobre los cortafuegos hardware Cisco PIX (Private Internet Exchange) y la tecnología ASA de Cisco. Comenta en detalle algún producto Cisco PIX.

# **Cisco PIX (Private Internet Exchange)**

**PIX** es el acrónimo de **P**rivate Internet E**X**change.

Esta sigla es utilizada por el fabricante tecnológico Cisco, para referirse a sus modelos de equipos Cortafuegos (FireWalls).

Se trata de un firewall completamente hardware: a diferencia de otros sistemas cortafuegos, PIX no se ejecuta en una máquina Unix, sino que incluye un sistema operativo empotrado denominado Finesse que desde espacio de usuario se asemeja más a un router que a un sistema Unix clásico.



El cortafuegos PIX utiliza un algoritmo de protección denominado *Adaptive Security Algorithm* (ASA): a cualquier paquete *inbound* (generalmente, los provenientes de redes externas que tienen como origen una red protegida) se le aplica este algoritmo antes de dejarles atravesar el firewall, aparte de realizar comprobaciones contra la información de estado de la conexión (PIX es *stateful*) en memoria; para ello, a cada interfaz del firewall se le asigna un nivel de seguridad comprendido entre 0 (la interfaz menos segura, externa) y 100 (la más segura, interna). La filosofía de funcionamiento del Adaptive Security Algorithm se basa en estas reglas:

- Ningún paquete puede atravesar el cortafuegos sin tener conexión y estado.
- Cualquier conexión cuyo origen tiene un nivel de seguridad mayor que el destino (outbound) es permitida si no se prohíbe explícitamente mediante listas de acceso.
- Cualquier conexión que tiene como origen una interfaz o red de menor seguridad que su destino (inbound) es denegada, si no se permite explícitamente mediante listas de acceso.
- Los paquetes ICMP son detenidos a no ser que se habilite su tráfico explícitamente.
- Cualquier intento de violación de las reglas anteriores es detenido, y un mensaje de alerta es enviado a syslog.
- Cuando a una interfaz del cortafuegos llega un paquete proveniente de una red con menor nivel de seguridad que su destino, el firewall le aplica el *adaptive security algorithm* para verificar que se trata de una trama válida, y en caso de que lo sea comprobar si del host origen se ha establecido una conexión con anterioridad; si no había una conexión previa, el firewall PIX crea una nueva entrada en su tabla de estados en la que se incluyen los datos necesarios para identificar a la conexión.

El cortafuegos PIX puede resultar muy complejo de gestionar, especialmente a los que provienen del mundo Unix, ya que como hemos dicho se asemeja más a un router que a un servidor con cualquier flavour de Unix; es por tanto recomendable consultar bibliografía adicional antes de trabajar con estos equipos. Una buena referencia puede ser [JF01], así como la documentación sobre el producto que está disponible a través de la web de Cisco Systems

# Tecnología ASA de Cisco

Los dispositivos Cisco ASA 5505 y 5550 son componentes centrales de la estrategia Self-Defending Network de Cisco Systems. Ambos dispositivos forman parte de una familia de dispositivos de seguridad de red multifunción que ofrece la amplitud y profundidad necesarias para proteger empresas de cualquier tamaño. Su defensa proactiva frente a amenazas evita que los ataques se extiendan por toda la red de la empresa, permitiendo a las empresas proteger varios segmentos de una red al mismo tiempo, lo que consolida la inversión en seguridad y minimiza la complejidad de las instalaciones y reduce los costes operativos.



Diseñado para proporcionar servicios de seguridad de alto rendimiento para entornos de ancho de banda de nueva generación, Cisco ASA 5505 ofrece una rendimiento de firewall de 150 Megabits por segundo (Mbps) y una rendimiento de VPN encriptado de 100 Mbps. También ofrece flexibilidad y protección de la inversión significativa mediante su diseño modular único,

ofreciendo una ranura de expansión para capacidades futuras. Además, el Cisco ASA 5505 puede funcionar como un cliente VPN de hardware para simplificar la gestión. Ofrece servicios VPN SSL acelerados a través de hardware, un switch de 8 puertos 10/100 integrado compatible con la creación de múltiples "zonas" de seguridad y dos puertos integrados de Power-over-Ethernet (PoE). Entre sus diversos usos, dichos puertos PoE ofrecen una instalación intuitiva y sencilla para teléfonos Cisco IP y puede proporcionar energía a puntos de acceso Cisco con la que se mejora la movilidad del usuario.

El Cisco ASA 5550 incluye el firewall de Cisco, líder del sector y los servicios IPsec/SSL VPN dirigidos a entornos de red para grandes empresas. Puede proporcionar más de 1,2 gigabits por segundo (Gbps) de rendimiento de firewall y da soporte a 200 redes de área local virtuales (VLAN), de modo que las empresas pueden segmentar su red en numerosas zonas de alto rendimiento para mejorar la seguridad. También ofrece servicios VPN escalables, que soportan hasta 5.000 clientes IPsec y SSL VPN por aplicación. Mediante sus capacidades de agrupación de VPN y de balanceo de carga, las empresas pueden agrupar hasta 10 dispositivos Cisco ASA 5550, dando servicio a 50.000 usuarios simultáneos de IPsec y SSL VPN.

Al ampliar el alcance de la familia Cisco ASA y aprovecharse de los nuevos servicios Cisco ASA Software 7.2, las empresas pueden ampliar la aplicación de seguridad a través de su red. Ofrece más de 50 nuevas opciones de seguridad que refuerzan el firewall de capa de aplicaciones de la familia Cisco ASA, VPN de acceso remoto, alta disponibilidad, integración de redes y capacidades de gestión. De estas mejoras, algunas de las más significativas son los servicios de firewall en la capa de aplicaciones y la integración de servicios con Cisco Network Admission Control (NAC). Los servicios de firewall en la capa de aplicaciones de Cisco proporcionan a las empresas un mayor control sobre sus dispositivos y ayudan a prevenir que las amenazas accedan a las redes empresariales. Además, mejoran la protección de protocolos de aplicaciones como web, correo electrónico, voz sobre Protocolo Internet (VoIP), mensajería instantánea, transferencia de archivos y protocolos de red Microsoft. El soporte de Cisco ASA para las soluciones NAC de Cisco administra evaluaciones integrales para usuarios y dispositivos que accedan a la red mediante conexiones IPsec y SSL VPN. Esta evaluación incluye la comprobación de las actualizaciones correspondientes de software de seguridad y sistemas operativos antes de conceder acceso a los privilegios en red.

# b) Elabora un informe sobre productos comerciales que implemente Gestión Unificada de Amenazas **"Firewall UTM"** (Unified Threat Management).

# D-Link Firewall UTM NETDEFEND

Firewall UTM para delegaciones

El firewall UTM DFL-260 ofrece una potente solución de seguridad para las oficinas de pequeño o medio tamaño, con hasta 50 usuarios, contra una amplia variedad de amenazas para la red en tiempo real. Al integrar un sistema de prevención de intrusos (IPS), un gateway antivirus (AV) y el filtrado de contenidos web (WCF) en un diseño industrial de tamaño de sobremesa, este dispositivo está dirigido a las empresas que buscan seguridad para la red a un precio competitivo.



Gestión de amenazas unificada

El DFL-260 integra un sistema de prevención de intrusos (IPS), un gateway antivirus (AV) y el filtrado de contenidos/URL web para una mejor protección con inspección de contenido de nivel 7.

Está disponible un servicio opcional de subscripciones para mantener actualizadas en tiempo real cada una de estas defensas.

## Potente prevención de intrusos

El DFL-260 sigue una única tecnología IPS, firmas de virus basadas en componente, que se integra para reconocer todas las variedades de ataques conocidos y desconocidos y proteger contra ellas, y que puede tratar todos los aspectos críticos de un ataque o potencial ataque, incluidos la carga, NOP sled, infección y exploits. En cuanto a la cobertura de las firmas de virus, la base de datos IPS incluye informaciones y datos de ataque procedentes de una parrilla de sensores global y, además, exploits recopilados de sitios públicos, tales como la National Vulnerability Database y Bugtrax. El DFL-260 cuenta con firmas de virus IPS de alta calidad porque constantemente crea y optimiza las firmas de virus NetDefend por medio del sistema sensor de autofirma de D-Link (Auto-Signature Sensor System). Sin sobrecargar el dispositivo, estas firmas garantizan una alta tasa de precisión de detección y la menor tasa de falsos positivos.

## Escaneado de virus basado en el flujo

El DFL-260 escanea archivos de cualquier tamaño utilizando una tecnología de escaneo de virus basada en el flujo que no requiere almacenamiento temporal. Este método de escaneado mejora el rendimiento de inspección al mismo tiempo que elimina los cuellos de botella en la red. El dispositivo usa firmas de virus de la respetada compañía antivirus Kaspersky Labs para proporcionar a los usuarios unas firmas antivirus precisas y fiables, así como comunicar las actualizaciones de firmas. Por consiguiente, se pueden bloquear con eficacia los virus y el malware antes de que lleguen a los dispositivos móviles o de sobremesa de la red.

## Filtrado de contenido web

El filtrado de contenido web ayuda a los administradores a monitorizar, gestionar y controlar el uso que los empleados hacen de internet. El DFL-260 implementa varios servidores de índice global con millones de URL e información de sitios web en tiempo real para mejorar la capacidad de rendimiento y maximizar la disponibilidad del servicio. El firewall usa políticas granulares y explícitas listas blancas y listas negras para permitir o denegar el acceso a determinados tipos de sitios web para cada combinación de usuarios, interfaces y redes IP. Puede desmontar los potenciales objetos maliciosos, como applets de Java, JavaScripts/VBScripts, objetos ActiveX y cookies, para tratar activamente el contenido de internet.

## Acelerador por hardware

El DFL-260 usa un acelerador por hardware para llevar a cabo las funciones de escaneado antivirus e IPS simultáneamente, sin que se degrade el rendimiento del firewall ni el de la red privada virtual.

Este potente acelerador le permite al firewall trabajar con un rendimiento muy superior al de los firewall UTM con función antivirus del mercado.

## Potente rendimiento de la red privada virtual

El DFL-260 dispone de un motor de red privada virtual basado en hardware para soportar y gestionar hasta 100 túneles VPN. Admite los protocolos IPSec, PPTP y L2TP en modo cliente/servidor y también puede manejar el tráfico que pasa a través de él. La autentificación de usuario puede llevarse a cabo por medio de un servidor RADIUS externo o a través de la base de datos interna del firewall, que admite hasta 150 cuentas.

## Monitorización y gestión

El DFL-260 puede gestionarse remotamente a través de la interfaz basada en web, la interfaz de línea de comandos por el puerto consola RS-232 o una conexión SSH (Secure Shell). La configuración es rápida gracias a un asistente de instalación que incluye características avanzadas para monitorizar la red y conservarla en buen estado y con total seguridad, tales como avisos por correo electrónico, registro del sistema, comprobaciones regulares y estadísticas en tiempo real.

## **Clavister Extended UTM**

Desde el principio, el requerimiento mínimo UTM era un Firewall, Detección de Intrusión de red (IDS) y funcionalidad de Prevención de Intrusiones (IPS), y Antivirus de Entrada (AV Perimetral). El último producto de Clavister ofrece esta funcionalidad junto con capacidades VPN, Control de Tráfico y Gestor de Filtrado de Contenidos, todos con capacidad de multi-gigabit. Lo llamamos xUTM. La demanda de dispositivos, al contrario de software, se explica por el aumento del requerimiento de la conveniencia plug & play, son de fácil instalación y de administración centralizada. Los dispositivos son más fáciles de desplegar que las soluciones de software, ya que incluyen su hardware y software pre-integrados. Son generalmente muy confiables y pueden resistir gran volumen de tráfico. La mayoría pueden tener más escala agregando más dispositivos. Cuando una maguina falla, es más fácil cambiarla que localizar el problema. Este proceso pone al nodo en línea más rápido, y puede realizarse por personal no técnico. Esto es especialmente importante para oficinas remotas o para las PYMES con poco personal capacitado.



## Integridad

## Oferta producto completo

Incluye todos los componentes necesarios para despliegue, administración y apoyo de su infraestructura de seguridad de por vida.

## El conjunto más variado

Incluye Firewall, VPN, Anti-virus, Prevención y Detección de Intrusión, Administración de tráfico, Control de Aplicación, Failover, Control P2P, Routing avanzado y mucho más.

## Ximark UTM/Firewall

La administración de Firewalls y UTMs es intensiva en recursos y requiere un alto nivel de conocimientos. Debido a la complejidad asociada a estas tareas, la mayoría de las violaciones son causadas por la incorrecta configuración de reglas y políticas de firewall.



Ximark UTM/Firewall Administrado es un servicio de administración de dispositivos de seguridad de perímetro, conocidos también como "Administradores de Amenazas Unificadas" que protegen a las organizaciones con

herramientas integrales como: anti-spam, anti-virus, sistema de prevención de intrusos (IPS), filtro de contenido web, control de "peer-to-peer" (P2P) y control de chat, entre otros.

El registro de eventos, la administración de la configuración y los reportes centralizados son fundamentales de acuerdo a las mejores prácticas de seguridad modernas. Con Ximark UTM/Firewall Administrado las organizaciones pequeñas y medianas pueden cumplir con estas prácticas. Con nuestro modelo de seguridad "On-Demand" las empresas de todos los tamaños pueden beneficiarse de una solución centralizada de administración y monitoreo de sus dispositivos de seguridad perimetral de varios fabricantes líderes. No hay requerimientos adicionales de hardware, software o facilidades, lo cual provee un costo competitivo.

## Funcionalidades del Servicio

## • Monitoreo

Administración de registros (logs). Revise registros en tiempo real o históricamente. Para diagnóstico o análisis de seguridad.

Monitoreo de la disponibilidad del dispositivo. Sea notificado cuando el dispositivo presenta problemas de desempeño o conectividad.

## Reportes

Servicio "On-demand". Acceda al servicio desde cualquier ubicación vía Internet vía un browser.

Reportes pre-configurados. Vea reportes de actividades como los hosts más activos, servicios más usados, sitios más visitados y otra información útil para diagnóstico y control.

## Administración

Administración de la configuración. La ejecución de cambios programados se incluye dentro Ximark UTM/Firewall Administrado.

Mantenimiento. Las tareas de mantenimiento como actualización de firmware y otras.

Actualización de servicios de protección. Los servicios de protección UTM como anti-spam, anti-virus, IPS y filtrado de contenido web se actualizan.

## • Mesa de Servicio

Mesa de servicio vía Web. Puede abrir casos 24x7x365 días al año vía web y por teléfono. Como un sólo punto de contacto para todas sus necesidades de soporte, nuestros ingenieros que atienden vía nuestra plataforma web, tienen experiencia en soportar redes y ayudar a diagnosticar problemas y proveer soluciones. La mesa de servicio permite que Ximark responda tan rápido como sea posible o de acuerdo a los acuerdos de niveles de servicio (SLA) establecidos con el cliente. Para ellos es posible manejar escalamientos y alertas a los gerentes del área de soporte. La mesa de servicio es basado en Web y en tecnologías de última generación. El sistema posee una base de datos conocimiento, calendario, manejo de SLAs, y otras funcionalidades que permiten brindar un servicio de soporte avanzado.

### • Niveles de Servicio

Ximark UTM/Firewall Administrado ofrece niveles de acuerdo de servicio (SLA) para garantizar la disponibilidad y confiabilidad.
