Enrotamento básico con Linux

Sumario

- 1 Introdución
- 2 Preparativos da MV drouter
- 3 Preparativos S.O. drouter
- 4 Configuración do servizo de routing sobre NAT
- 5 Configurar a porta de enlace dun cliente da LAN
 - 5.1 Probas de conectividade

Introdución

- Imos crear un escenario que faga uso dun router, implantado cunha MV, que permite dar saída a internet ás demais MVs e ademais así cada MV só precisa ter un adaptador, conectado a unha rede interna.
- Preténdese instalar e configurar un router en Debian, de xeito que este faga de pasarela para os equipos da rede interna (*wserver*, *dserver*, *wclient*, *uclient*, etc).



- Este equipo, como router, terá 2 interfaces:
 - Interface LAN: para poder comunicarse cos equipos da LAN e viceversa. A IP desta interface será a porta de enlace que deberá configurar todo cliente da LAN.
 - Interface WAN: co que este equipo se vai comunicar co exterior. Ademais cando se configure o servizo de routing vaise configurar NAT nesta interface, para que calquera solicitude de conexión co exterior que parta dos equipos da LAN sexa transformada cara o exterior como se fora este equipo (drouter) que a fixera. Ao recibir a resposta do exterior vaise encargar de enviarlla ao equipo da LAN que iniciou a conexión.



Para revisar e afondar no coñecemento sobre NAT pódese consultar:

- NAT da parte III do presente curso.
- Antes de comezar a implantar o escenario, obsérvese que só se vai configurar **drouter** e **uclient**, os demais equipos enténdese que o usuario sería quen de configuralos, pero irase facendo pouco a pouco cando se precisen.

Preparativos da MV drouter

- Antes de configurar o servizo de routing vaise configurar a MV que o implantará:
 - Clonar a MV Debian, que teña xa o servizo de ssh e o Webmin instalado.
 ◊ Nome MV: drouter.
 - Facer unha instantánea.

Adaptador 1 Adaptado	r 2 Adaptador 3 Adaptador 4	
🖉 Habilitar adaptador	de red	
<u>C</u> onectado a:	NAT *	
Nombre:		\$
♥ Avanzadas		
<u>T</u> ipo de adaptador:	Intel PRO/1000 MT Desktop (82540EM)	:
Modo gromiscuo:	Denegar	\$
Dirección MAC:	080027A778D7	
	Gable conectado	
	Reenvio de puertos	

Configurar o adaptador 1 por NAT, e asegurarse de que o enderezo MAC non é o mesmo que o da MV da que se clonou.

Red		
Adaptador 1 Adaptador	2 Adaptador 3 Adaptador 4	
🖉 Habilitar adaptador d	le red	
<u>C</u> onectado a:	Red interna 🔹	
Nombre:	intnet	
🗢 Avanzadas		
Tipo de adaptador:	Intel PRO/1000 MT Desktop (82540EM)	\$
Modo promiscuo:	Denegar	4 T
Dirección MAC:	0800278£878C	
	☑ Cable conectado	
	Beenvio de puertos	

Configurar o adaptador 2 por Rede Interna, e asegurarse de que o enderezo MAC non é o mesmo que o da MV da que se clonou.

Preparativos S.O. drouter

- Antes de instalar o servizo de routing, configuraranse as interfaces de rede.
- Preparación de máquina drouter



Agora no sistema aparecerán dúas interfaces de rede, co nome *eth0* e *eth1*. Podemos velas co comando **ifconfig -a**, e nos fixaremos nas súas direccións MAC para saber cal é a interface conectada en modo interna e cal é a NAT. Neste caso, *eth0* é a interface en modo NAT e



Debemos configurar a interface NAT de forma automática por DHCP e a que está en rede interna coa dirección 172.16.0.1. Podemos facelo de calquera das formas xa vistas no curso, na imaxe móstrase como facelo utilizando o ficheiro de configuración das interfaces en Debian.

root@ds	erver:/home/dadmin# service networking restart erver:/home/dadmin# ifconfig
eth9	Link encap:Ethernet HWaddr 08:00:27:a7:78:d7 inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0 inet6 addr: fa00::a00:27ff:fea7:78d7/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:17 errors:0 dropped:0 overruns:0 frame:0 TX packets:325 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:2488 (2.4 K18) TX bytes:93243 (91.0 K18)
ethl	Link encap:Ethernet HWaddr 08:00:27:be:87:8c inet addr:172.16.0.1 Bcast:172.16.255.255 Mask:255.255.0.0 inet6 addr: fe80::a00:27ff:febe:878c/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:8 errors:0 dropped:0 overruns:0 frame:0 TX packets:53 errors:0 dropped:8 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:0 (0.0 B) TX bytes:24449 (23.8 KiB)

Tras gardar os cambios no ficheiro, reiniciamos o servizo de rede para aplicar a nova configuración. Comprobamos co comando **ifconfig** que as interfaces están configuradas cos novos datos.



Comprobamos con ping que a máquina ten conexión con www.google.es.

Configuración do servizo de routing sobre NAT

• En Linux, o protocolo NAT configúrase como unha regra dentro do servizo do Firewall. Para poder configurar este servizo de forma sinxela, instalaremos a aplicación **shorewall**. Webmin inclúe un módulo que nos permitirá configurar de forma gráfica todo o comportamento do Firewall e do procolo NAT.

Lagre root	Ayuta. Configuración de Módulo			Paquetes de Software
> Webman	Paquetes Instalados			
** Solena Anangue y Parada	Buscar Pagartec			
Autoriticación PAM Camileo de Contraseñas	Instalar Nuevo Paquete			
Convestos Planificados Copia de Segundad de	Seleccors is localización desde de	exterentialar el pagaete DPR-G	l de Debian	
Sistema de Archivos	C Deade antibivo local			
Hutorce (Logi) del Saterna MIME Type Programa	O Deade antitivo cargado	Newgar., Nevgan Sche	ro seleccionado	
Pagatas de Soltware	C Deade direction URL Np o http	P		
Processos en curso Páginas del Manual	® Paquete deode APT	shorewall	Buscal APT	
Retación de Hestinicos (Logn)	instalar.			
y Red	Identificar un Archivo			
Software Package Updates	hand been as successful to be been		an in here of a matter formed, as	Delter
Unumine y Crupon	recontra el consiste o la reject	one de un archivo donde buoc	of the basic of dation Device de	Depter
Earvidores	Butcie:			

Utilizamos o módulo de Paquetes de software da categoría Sistema do Webmin para instalar o paquete shorewall.



Unha vez instalado o paquete, utilizamos a opción de **Refrescar módulos** para que se mova o módulo de xestión de shorewall á categoría que lle corresponde.

Configur	Configuración de Red	
1		Concession of Magnet
e rese tantit pass activar in historiane de Merupi de arrang	and the interface water and a state actual had been serial designed in	
r com texte para activar la interface de temps de arrang manimentale datria la mei y come altactante a dataser.	te 1 e coultanae e seo ever je com acer este estructu	na menan Advantance composite deprint to

En primeiro lugar imos activar o servizo de enrutamento. Dentro da categoría de **Rede** imos ao apartado de **Configuración de rede** e picamos sobre **Enrutamento e portas de enlace**.

Router por defecto	· Ningan	a lo desde DHCP1	Cabreau	eth0 ±	
Actuar como router?		8		1000.41	
Rutas estáticas	Intertaz	Red	Máscara de red	Gateway	
Rutas locales	Interfac	Red	Mar	cara de red	
Salvar					

Activamos a opción de Actuar como router e gardamos os cambios.



Na páxina principal do módulo de configuración da rede, picamos no botón de **Aplicar configuración** para activar os cambios realizados. Pero neste caso (debido a un *bug* do webmin) con isto non conseguimos realmente activar xa o servizo de routeo na máquina. Se reiniciásemos a máquina virtual xa se activaría, pero imos ver como podemos activar o cambio sen ter que reiniciar.



No propio webmin, imos á ferramenta de **Comandos de consola** (dentro do apartado de **Outros**) e introducimos o comando: **sysctl -p**. Picamos no botón de Executar comando para executar este comando no sistema.

	Comandos de Consola	
· sysatti ·p		
eet.spot.sp.formere + 1		
ended on a content of colored at the specific at its copy in t	tota minera El mamante de la puede una para instituir de antenne a se oparetes comantes.	
Epectar consents		Lorgen taland

Vemos o resultado do comando, que xa activa o enrutamento.

ingen inte	Configuration in Frank	Constuego	s Shorewall	Band Decourse.
Import I			The second secon	Right in a reflection of the second s
Contrast Contra Neuroperations Neuroperations Contrast Co	international and international comparation of contractions international	Pearse can man particul Mediati no collegiono Pearse can man particul ga francar can do origine Can do data o na Tanana rang derimar turk o	nan sekara dara dara kura (ali ana kara dara kura kura kura (kura kura) kura (kura kura)	

Imos agora activar o protocolo NAT, para o que faremos uso da ferramenta **Cortafogos shoreline** que atopamos na categoría de **Rede** do Webmin. Na páxina principal, veremos que aparece o botón de **Iniciar o cortafogos** porque neste momento o servizo está parado. Antes de poder inicialo, temos que establecer unha configuración básica para que funcione correctamente. Picamos en primeiro lugar na opción de **Zonas de rede**.

Indexe de Mastala	Zonas de Red
Lie Done: Theirs or with pages repre-	antar alamine was accepted ande to coloria. No alcosta, non emissio is term angle more color a colatingia - emperants administratory associations de loria
Tortori, so se la definite singure co	
Sprige also merce, case de real.	
Lillia el Tactoro Manuelmente	Presse era lotti pes ella navaltera a lotti chi vez vezi conte la Domal, delle sulle partete la ereste in arte.
· Copera a los acosos	

O obxectivo das zonas de rede é proporcionar un nomo lóxico ás distintas redes ás que está conectado este sistema, para así xestionar o firewall de forma máis sinxela. De momento vemos que non hai ningunha zona creada, así que imos crear unha nova.

Se nos fixamos no escenario, podemos ver a *drouter* está conectado a dúas redes, unha rede interna (lan) e outra externa (wan). Así que imos crear dúas zonas de rede para representar estas dúas redes. Para crear unha zona basta con poñerlle un nome, neste caso *lan*. Como tipo de zona seleccionamos *IPv4*.

tration de Windom		Zonas	de Red		
an come branks, or other pag	parapeterize diserted table al-out	no ana is stored. No polaris, mias at	rate a rese may rest a state	property and a state of	enters y transpission in Law
Intercome tont y manter and	title (Apage on Land Inte & M.				
ID IN ADDA	Parent area	Down type	Dermant	Despisor	main
Det .		1718			¥.4
140		1748		**	TL
Cest		Consult subtract		*	Y A
Little of Forball Monument	n People and bein po	Letter remainence a fultery hold/later	reality over an interest, sends of	la-portation intervention de perfora	
Lan all the second	Property and india and	a setting responses on the large bala children	and in the second starts of	or exercising by provides in order.	
· improve a loss of losses,					

Da mesa maneira creamos a zona *wan*. É obrigatorio tamén crear unha zona que represente ao propio equipo, para logo poder definir regras no firewall para conexións que saian ou cheguen a esta propia máquina. Neste caso, a esta zona chamámoslle *sist*, e debe ser de tipo *Firewall system*. Regresamos á lista de táboas para seguir coa configuración do firewall.



Imos entrar na opción de Interfaces de rede para indicar cales son as interfaces de rede sobre as que acutará o firewall, e a que zona de rede está conectada cada unha delas.



Veremos que non hai definida no firewall ningunha interface de rede, así que agregamos unha.

	Crear Interfaz de Red				
	Recting in case				
Hears - National - Statement over 3842 P Hears an operating road through Hears an operating road through Hears and operating road through Hears and operating road through Hears and the regulation for any Table regulation for any	nu	Angene Angene proses of package Angene man and the second Angene man and the second Angene man and the second Angene and the second and the Angene and the second and the Angene and the second and the		Straging Hull Ngentreen Chees testage 102 Fage Accept table back to real Chees tertespatial source parkets	
	The second secon	Bestime Meetidee de como Persigner (*) Autoritation (*) Persigner (*)	Meetings Periodice its come Periodical constantion Periodical constantion Periodical constantion Periodical constantion Periodical constantion Periodical constantion	Perspective Number of water mm Perspective Sectors of the sec	

Para crear unha interface de rede no firewall, debemos introducir o nome dunha das interfaces de rede do equipo (que será do tipo *eth0*, *eth1*, *wlan0*, etc.) e seleccionar á zona de rede coa que está conectada esta interface. Por exemplo, no noso caso a interface *eth0* está conectada é zona wan Croames a interface

the state		Interfaces de	Red		
Demographic deb	en este triter y talk one de las interferes	for net oil signature part passes part (forward particula, non	take on is one of is parents' could	inter 14 contacts in teachers in	the last species
Andrews India (1	beenth uniterative. Agengar and hanna hand	ter de mil			
mantal	Numbers do passa	Direction in Annual and	Opennie	despite/a	1000
Comp	-	Magne	The general sector of the sect	*	TA
C and	-	Magaza	The party		TA
follow of Fallers 1	faturitaria international	nin privatio manaferito d'interventi.	Lobertheory in Decemal. Much rolling	particles in estimate in price	
Rolling of Walters -	Refer one	the period is a subsection of the sector of the subsection	Collection in the second second second		
Increase a lists	the failure				

e da mesma maneira engadiríamos a interface *eth1*, neste caso conectada á zona *lan*. Como *drouter* só ten dúas interfaces de rede, xa están todas definidas e regresamos á lista de táboas.

Configuration in Manho	Contailuege	Contatuegos Shorewall				
Anna a far	THE CONTRACT OF THE CONTRACT.		Frages de Canadarque			
TOS		33	.490.1 2.345b			
			and the second			
	4	?	1			
Innue et constraigen Innuesen et Constraigen Noom Innue	Process con tests pay along Strongel (or is only proce- Process and tests pay how an Messad value is enlight tools to below a new Messad range formation for the	etais ole la argen ator secci (1947) alute car la argen stor escit, check, for sacti daga catoriana.				

Para rematar, temos que definir as políticas por defecto do firewall, que son os criterios básicos que o firewall utiliza para decidir se acepta ou rexeita as conexións. Estas políticas poden ser refinadas de forma máis específica mediante *regras*, en función das máquinas de orixe ou de destino das conexión ou o protocolo que se utilicen na mesma, pero neste curso non imos afondar máis na xestión do firewall.

trates in Ander	P	oliticas por Defecto	
tra papa pereir cathpra las accere	a per colocce para el techos error paras efferentes ant car	alarge. Parke or petrolarizes per order tare o	t tan mit tahun mi sa pagina da majau dar Contaburgen
factures no serile definitio rangeno petiti	tra per adicto.		
Aprepti and makes perform per ordering			
Edite of Lines Management	Parana advisiti per ella mendence d'hire	en veta catar meditory at tag de Microsoft, davie pala	r purisits in estudie in othe
· Peyron a hole in Lation			
		a alafiniala aní avez in	
vemos que non	nai ningunna politic	a definida, así que in	nos crear unha nova.
Indice de Modulo		Creación de Politica por	Defecto
Detaillans de la portitiva por defecto			
Zona origen	-Custoverar 2	Zona destino	«Cualquera»
Politica	ACCEPT	Most de systog	«Heddrein desachvados» 🛔
Limite de tráfico	It Magano C Limite	st(Explored)	
Court			
· Represe a tieta de políticas			

Basicamente, para definir unha política deberemos indicar a zona de orixe e de destino dos paquetes aos que se aplicará a política, e a decisión a aplicar que fundamentalmente pode ser **Aceptar** (*ACCEPT*) ou **Borrar** (*DROP*). Para simplificar todo o posible a configuración do firewall, imos crear unha política que acepte todas as conexións, veñan da zona que veñan e vaian á zona que vaian. Isto non sería unha configuración desexable nun caso real, xa que facilitaría ataques externos á nosa rede, pero como se dixo non se pretende afondar na xestión do firewall.

million on shoese		Po	viticas por Defecto		
Cate plays a permit configuration	antes pe delera per eleter	arise prises afferentess dat-com	forgin. Poster on periodelocies pro-	riette ferri a ipo de infine e la pagra de es	ini in Cristingen
Solocycene tais, (heren's solocyce	a hyanga' ana mana pakita pir i	anco			
Zama origan	Two dates	Particula	Marci de lapolog	Longillo de Inalisco	Num
Chiumperte	Concerns	ADDPT	Newports	tergate	TA
· Segme a laboration					

Vemos na imaxe a política creada. Regresamos a lista de táboas, para iniciar xa o servizo do firewall.



Coa configuración establecida xa podemos inciar o cortafogos, picando sobre o botón.



Saberemos que o servizo está iniciado porque os botóns da parte inferior da páxina cambian, para mostrar opcións que só están dispoñibles cando o firewall está en execución. Quédanos por ver como utilizar este módulo para configurar o protocolo NAT. Picaremos na opción de **Enmascaramento**. Dáselle este nome ao protocolo NAT porque o que fai é *enmascarar* as direccións dunha rede privada a través da dirección IP pública do router.

testes de Minhala	Enmascaramiento
Los intendes de esta página configurari	a haducción de direcciones de red para el indice encaminade entre alguna red y una intenfaz particular.
Todavis no se ha definido ningana ne	de enmascaramiente.
Ageiger una nueva regla de menanciatar	Auto a sea constant,
Eater of Fichers Manualments	Presse est toto pas ella mavaltette il fichen /st1/shcrews12/sasq & thoreal, doub este guedata la estada di arte
· Megence a loca de tables	
Veremos que no	n hai ningunha regra de enmascaramento creada, así que o
Veremos que no	n hai ningunha regra de enmascaramento creada, así que o Crear de Regla de Enmascaramiento
Veremos que no	n hai ningunha regra de enmascaramento creada, así que o Crear de Regla de Enmascaramiento
Veremos que no	n hai ningunha regra de enmascaramento creada, así que Crear de Regla de Enmascaramiento
Veremos que no rece a Mater Destre de la reja de exercica tenera de subla	n hai ningunha regra de enmascaramento creada, así que o Crear de Regla de Enmascaramiento
Veremos que no reco e total festes de total testes de total	n hai ningunha regra de enmascaramento creada, así que o Crear de Regla de Enmascaramiento
Veremos que no trato de Maser Destina de la regia de elementar Red a elementar Red a elementarian	n hai ningunha regra de enmascaramento creada, así que o Crear de Regla de Enmascaramiento
Veremos que no reco a totale banta de la regia de concerto territor de calita de concerto de calita de concerto de calitad	n hai ningunha regra de enmascaramento creada, así que Crear de Regla de Enmascaramiento
Veremos que no relación de Minister Deserter de la regia de senacion tenerter de senacion Media esemacione Desección SMAT Resecto to protecel	n hai ningunha regra de enmascaramento creada, así que o Crear de Regla de Enmascaramiento
Veremos que no trace de Mateix Destructor de la regla de exercica Red a consecuenta Red a consecuenta Dirección Stati Reservici to profeso Reservici to profeso	n hai ningunha regra de enmascaramento creada, así que Crear de Regla de Enmascaramiento

O importante é seleccionar a interface de saída, que é a que ten a dirección IP pública es está conectada á rede WAN (que neste caso é **eth0**) e marcar como rede a enmascaras a que está conectada á interface que ten a dirección IP privada (neste caso **eth1**). Creamos a regra.

India di Mistari	Enmasce	wamiento	
in strain is not pigna tellpast to	Instantio de directores de vergen, d'odice-enacionale entre algais e	nt p and relative particular	
Administer Salls Inventor sales are Ay	reparate to the region of the second se		
transfer the section	Red a company	Breaster Staff	Allowed to
0.000	Hand and off Hit.		T L
detailant talk (Interfe selection (Ag	pegar sen rusmo regla de protacoarateristo (Auli a non constante).		
Damas Specified			
Dates of Politics Harvallenite	Presidine administrativ pass relian manufamente at fortensi -rol to rol-or	nall/Anny to Morenal, Bretto estas populates nel attendo	e in artis.
A Property of State or Surger			

Podemos ver a regra creada, que enmascara a rede conectada a *eth1* sobre a interface *eth0*. Con isto xa estamos proporcionando a información necesaria para facer NAT. Regresamos á lista de táboas...



e tan só temos que aplicar a configuración.

Configurar a porta de enlace dun cliente da LAN

- Para mostar a configuración da porta de enlace nun cliente da LAN vaise escoller a MV uclient; nos demais equipos a filosofía sería a mesma.
- Configurar a porta de enlace dun cliente da LAN

Adaptador 1 Adaptador	r 2 Adaptador 3 Adaptador 4	
Babilitar adaptador	de red	
<u>C</u> onectado a:	Red interna 🙏	
Nombre:	intret	
♥ Avanzadas		
Tipo de adaptador:	Intel PRO/1000 MT Desktop (82540EM)	
Modo gromiscuo:	Denegar	
Dirección MAC:	08002708A00B	6
	Gable conectado	
	Reemón de puertos	

Configuramos un só adaptador en modo Rede interna.

ome da conexión: Co	onexión cablead	la 2		
Keral Cableada Seg	uridade 802.1x	Config	uración IPv4	Configuración IPv
Método: Manual				×
Enderezos				
Enderezo	Máscara de re	de Pasarela		Engadir
172.16.0.140	255.255.0.0		172.16.0.1	Eliminar
Servidores DNS:	8.8.8.8			
Dominios de busca:				
ID do cliente DHCP:				
Para completar	a conexión requ	irir un e	nderezo IPv4	
				Camiños

Configuramos a IP segundo o escenario: 172.16.0.140/16, porta de enlace 172.16.0.1 (drouter, pola interface LAN).



Con **ifconfig** comprobamos que a configuración establecida está activada. De non estalo, desconectamos a tarxeta de rede e conectámola de novo.

Probas de conectividade

- Para comprobar que todo está correcto pódense facer pings entre os distintos equipos do escenario.
- Neste caso vanse amosar exemplos de conectividade realizados dende uclient e que en moitos casos teñen que atravesar drouter.
- Probas de conectividade



A imaxe amos o resultado de facer ping a *drouter*, á dirección IP do host, á dirección IP do router físico que da a saída a Internet, a unha dirección IP en Internet (8.8.8.8) e a un servidor de Internet polo seu nome (*www.google.es*), obtendo resposta en todos os casos. A opción

-c 1 indica que faga un só faga unha solicitude de eco.



Se queremos comprobar que os paquetes están pasando realmente por *drouter* podemos instalar o paquete **traceroute**, que mostra os routers polos que pasa un paquete para chegar a un destino determinado.



Na imaxe vemos o resultado de executar **traceroute -n 8.8.8.8**, que mostra os routers intermedios (a opción -n é para que só mostre as direccións IP deses routers) ata chegar ao equipo coa dirección 8.8.8.8. Vemos marcado como pasa por *drouter* en primeiro lugar e logo polo router físico que da saída a Internet.

C:\Use	182.1	uadmin.	>tri	ace:	rt -d l	8.8.	8.8
Iraza	a 8.	8.8.8	sol	bre	canin	os d	e 38 saltos como náximo.
	(11*66**7887 12887		<11*5467788 1167788 17 12887		00*************************************		172.16.0.1 10.8.2.2 Tiengo de espera agotado para esta solicitud. 87.235.0.10 172.29.56.10 172.29.56.10 172.29.56.109 212.165.147.45 212.165.147.45 212.165.22.109 214.232.109 216.239.40.133
Iraza	com	pleta.					
C:\Use	150	wadmin)	>_				

Esta imaxe mostra o comando equivalente en *wclient*, que sería **tracert -d 8.8.8.8**. Como vemos, tamén se mostra como os paquetes pasan por *drouter* e polo router de saída a Internet.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez --