Balanceo de carga y redundancia entre dos ISP con PFSense y MultiWAN

En muchas organizaciones es vital no perder la conexión a internet en ningún momento. Por lo cual en los departamentos IT se suele contratar dos proveedores diferentes de internet o más. A continuación mostraré el procedimiento para implementar un sistema multi WAN con balanceo de carga y redundancia que tiene la ventaja de que si se cae un proveedor todo el tráfico sea redirigido por el ISP activo y a su vez si ambos funcionan correctamente, dividir todas las conexiones salientes por ambos servicios. Para ello utilizaremos un firewall basado en la distribución PFSense 2.0.

Para comenzar con el ejemplo, muestro un esquema con el escenario propuesto:



En resumen contamos con:

2 Proveedores de internet (ISP) diferentes.

1 Firewall implementado mediante PFSense 2.0 y con tres placas de red.

1 LAN Interna conectada a nuestra organización.

Para comenzar con la configuración, una vez instalado el SO PFSense, debemos asignar a cada una

1

de las interfaces una conexión.

Para ello vamos a **Interfaces** \rightarrow **assign** y configuramos la conexiones WAN1, WAN2 y LAN. Es decir definimos que placa se va a conectar a que servicio.



Se nos muestra la siguiente pantalla donde se realiza la asignación:

[®] Sense ,	 System 	 Interfaces 	Fir	ewall)	Services	•	VPN	•	Status	 Diagnostics 	×	Help	he geronet-	firewall
	Interface	s: Assig	n netw	ork po	ts								6 0	
	Interface assign	nments In	terface Gro	ıps Wirel	ess VLANs	s QinQ	s PPP	s GRE	GIF	Bridges LAGG				
	Interface			Netwo	ork port									
Concession in the	WAN1			em0 (00:0c:29:00:ad	:b1) 💌								
and the second second	LAN			em1 (00:0c:29:00:ad	i:bb) 🔻	\leftarrow	_						
and the second second	WAN2			em2 (00:0c:29:00:ad	:c5) 🔻	\leftarrow							

Una vez definidas las interfaces se debe indicar la IP de cada placa desde el menú Interfaces e ingresando en cada dispositivo:



En nuestro caso: IP Placa WAN1: 10.0.1.2, WAN2: 10.0.2.2 y LAN: 192.168.2.1

Luego debemos definir nuestros Gateway. En nuestro caso asignaremos las direcciones provistas por nuestros ISP (En el ejemplo: WAN1: 10.0.1.1 y WAN2: 10.0.2.1).

Para ello vamos a System → Routing



Pulsando en el signo (+), agregaremos los Gateway:

Edit gatew	av									
Interface	WAN1 Choose which	terface this gateway applies to.								
Name	NAN1G Gateway nam									
Gateway	I 0.0.1.1 Gateway IP a	iress								
Default Gat	teway Default This will sele	Default Gateway This will select the above gateway as the default gateway								
Disable Gat Monitoring	teway Disable This will cons	Gateway Monitoring Jer this gateway as always being up								
Monitor IP	10.0.1.1 Enter an alter as the load b	Alternative monitor IP ative address here to be used to monitor the link. This is used ancer entries. Use this if the gateway does not respond to ICI	d for the quality RRD graphs as well MP echo requests (pings).							
Advanced	Advanced	Advanced - Show advanced option								

En el campo Monitor IP debemos ingresar la dirección de un equipo que responda al comando PING. Este puede ser el router del ISP o algún DNS público. Esto se utiliza para determinar si el línk se encuentra activo o no.

Debemos agregar de la misma forma los dos gateway:

Sense	► System ►	Interfaces > F	irewall > Services	► VPN ► S	tatus 🕨 Diagnostics 🕨	Help 🐉 geronet-f
	System: Ga	teways es Groups				9 0
	Name	Interface	Gateway	Monitor IP	Description	G.
	WAN2GW	WAN2	10.0.2.1	10.0.2.1	GW WAN2	
	WAN1GW (default)	WAN1	10.0.1.1	10.0.1.1	GW WAN1	
						E

El siguiente paso es definir un Grupo de Gateway que en una misma conexión contará con nuestros dos Gateway provistos por nuestros ISP y se encargará de proveernos la salida a internet.

Para ello vamos a **Systems** \rightarrow **Gateway** \rightarrow **Groups**:

System	 Interfaces 	Firewall	→ VPN →	Status	 Diagnostics 	 Help 	않e geronet-f			
System: G	ateway Grou	ıps					60			
Gateways Routes Groups										
Group Name	Gateways	Priority	Des	cription			æ			
MultiWAN	WAN2GW WAN1GW	Tier 2 Tier 2	Multi	WAN Group		6				

Pulsando (+), accederemos a la pantalla para configurar el grupo:

Edit gateway entry	
Group Name	MultiWAN Group Name
Gateway Priority	Tier 2 • WAN2GW - GW WAN2 Tier 2 • WAN1GW - GW WAN1
	The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted we will use the next available link(s) in the next priority level.
Trigger Level	The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted we will use the next available link(s) in the next priority level. Member Down When to trigger exclusion of a member

Debemos asignar un nombre de grupo, en el ejemplo lo llamamos: MultiWAN.

Luego en el campo Gateway Priority nos aparecerán las pasarelas definidas en el paso anterior.

Por lo que en ambos casos debemos asignarle a cada una un Tier.

Para esto vamos a Firewall → Rules

<u>Importante</u>: si asignamos el mismo **Tier**, el sistema realizará un balanceo de carga de las solicitudes y no dará prioridad a ningún ISP en particular. En cambio si a uno le asignamos un Tier 1 y a otro un **Tier2**, el sistema priorizará al que tenga **Tier1** y sino está disponible, entonces luego redirigirá el tráfico por el ISP con **Tier 2**.

Una vez definido esto, debemos especificar una regla de ruteo de las solicitures.

Sense	→ System → Interfaces	✓ Firewall →	Services
		Aliases	
		NAT	
	System: Gateways	Rules gatewa	y
		Schedules	
	Edit gateway entry	Traffic Shaper	
	Group Name	Virtual IPs	
		Group Name	

Debemos agregar la regla que nos permita redirigir el tráfico saliente a nuestro grupo MultiWAN definido anteriormente:

[®] Sense /	 Syst 	em	► Interf	iaces → F	Firewall	 Services 	×	VPN D	Status	▶ Diagno	ostics	 Help 	片 geronet-fi
	Firew Floatin	vall: g (w/	Rules	WAN2	5YNC								600
		ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Desc	ription	œe
			*	*	*	LAN Address	80	*	*		Anti- Rule	Lockout	2 7 Fi
	0		*	LAN net	*	*	*	MultiWAN	none		Defai LAN 1	ult allow to any rule	
			тср	*	*	*	*	*	none		TEM	PORALLLL	
	D pas	s s (disab Rules block	led) are evaluati rules, you'll	ed on a first-ma have to pay att	tch basis (ention to t	ock ock (disabled) i.e. the action of th he rule order. Even	e first rule ything that	e to match a pa t isn't explicitly	reject reject (disi icket will be e passed is blo	abled) executed). This ocked by defaul	means t t.	that if you use	log (disabled)

Pulsando el botón (+) agregaremos nuestra regla de ruteo:

h the ect is ock th	the criter	ria snecifie					
h the ect is ock th	the criter t is that t	ria specifie					
	x the pat	with rejec cket is dro	ed below. t, a packe opped silen	t (TCP RST or tly. In either	r ICMP por case, the c	t unreacha original pao	able for UDP) cket is
remo	moving i	t from the	e list.				
ome i	ne in to r	natch this	rule.				
match 72 he	atch. here.						
e ma	match.						
-	-						
not Use this option to invert the sense of the match.							
Ŧ	1						
e mai	match. 	e rn on logg	ging	for ev	for everything. If y	for everything. If you want to	for everything. If you want to do a lot c

En este caso indicamos que permitiremos todo el tráfico saliente desde nuestra LAN a internet por medio del Gateway **MultiWAN**:

Description	C Default allow LAN to any rule You may enter a description here for your reference.
Advanced features	
Source OS	Advanced - Show advanced option
Diffserv Code Point	Advanced - Show advanced option
Advanced Options	Advanced - Show advanced option
State Type	Advanced - Show advanced option
No XMLRPC Sync	Advanced - Show advanced option
Schedule	Advanced - Show advanced option
Gateway	MultiWAN default WAN2GW - 10.0.2.1 WAN1GW - 10.0.1.1 wan1GW - 10.0.1.1
In/Out	Advanced - Show advanced option
Ackqueue/Queue	Advanced - Show advanced option
Layer7	Advanced - Show advanced option
	Save Cancel

De esta forma todas las peticiones a internet se redirigirán por nuestro grupo de Gateway y el

sistema se encargará de realizar el balanceo de cargas y redirigir el tráfico cuando uno de los dos ISP no se encuentre activo.

Finalmente nos será útil realizar el monitoreo del estado de los enlaces.

Para ello vamos a: Status→ Gateways

& Sense	► System ► Interfaces	Firewall ► Services ► VPN	Status Dia CARP (failover)
	Firewall: Rules: Ed	it	DHCP Leases Filter Reload
	Edit Firewall rule		Gateways
	Action	Pass Choose what to do with packets that match the criteria Hint: the difference between block and reject is that wit is returned to the sender, whereas with block the packet discarded.	Interfaces IPsec Delaw Load Balancer The e OpenVPN
	Disabled	Disable this rule Set this option to disable this rule without removing it fr	Package Logs Queues
	Interface	LAN Choose on which interface packets must come in to mat	RRD Graphs Services
	Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.	System Logs Traffic Graph UPnP & NAT-PMP
	Courses		

En la siguiente pantalla podremos apreciar el status de cada link:

Sense	 System 	▶ Interfaces	 Firewa 	ll 🔹 🕨 Ser	vices 🕨	VPN	 State 	tus Diagnostics	•	Help	🗧 geronet-fir
	Status: G	ateways	1								0
	Name	Gateway	Monitor	RTT	Loss	Status		Description			
	WAN2GW	10.0.2.1	10.0.2.1	0.478ms	0.0%	Online		GW WAN2			
	WAN1GW	10.0.1.1	10.0.1.1	0.311ms	0.0%	Online		GW WAN1			

Espero, les sea útil.

Saludos.