# Configurar un firewall con failover en PFSense 2.0.1

Básicamente la idea consiste en configurar en nuestra organización un firewall con redundacia en la cual se replican los estados de las conexiones en un equipo de backup y en caso de producirse una falla en el principal, el secundario entre en funcionamiento automáticamente sin producir cortes en las comunicaciones.

Por ello en el ejemplo configuraremos dos firewall capaces de funcionar sincronizadamente, uno como equipo principal y otro como secundario de backup.

Nuestro esquema propuesto es el siguiente:



Elementos necesarios.

- 1 Proveedor de internet que nos proporcione tres IP para conectarnos a la red.
- 2 Equipos que funcionen como firewall y PFSense 2.0 instalado.

- 3 Placas de red en cada firewall.
- 1 dirección IP VHID definida para la red WAN.
- 1 dirección IP VHID definida para la red LAN (esta será el gateway para los clientes de la LAN).

Las direcciones VHID son las direcciones IP virtuales que serán compartidas por los firewalls para establecer las conexiones tanto en la LAN interna como en la WAN. Es decir, ambos equipos responderan a la misma IP, sin embargo tambien cada equipo debe tener su dirección particular.

En resumen en cada equipo configuraremos las siguientes direcciones en cada placa:

### Firewall 1 (Principal):

WAN: 10.0.1.2

LAN: 192.168.2.1

SYNC: 1.1.1.1 (Será la IP utilizada para sincronizar los firewalls)

### Firewall 2 (Backup):

WAN: 10.0.1.3

LAN: 192.168.2.2

SYNC: 1.1.1.2

Y a su vez, en <u>ambos</u> equipos las siguientes IP Virtuales:

VHID WAN: 10.0.1.250 (Debe ser provista por el ISP)

VHID LAN: 192.168.2.250 (Será el gateway al que deben aputar los clientes)

Comencemos entonces con la configuración:

Primero asignamos las placas de red a las diferentes interfaces desde el menú Interfaces -> Assing

*Sense	► System ► Interfaces ►	Firewall   Services   VPN   Status   Diagnostics	<ul> <li>Help</li> </ul>	밝• geronet-i
	Interfaces: Assign net	work ports		80
	Interface assignments Interface G	roups Wireless VLANs QinQs PPPs GRE GIF Bridges LAGG		
	Interface	Network port		
	WAN1	em0 (00:0c:29:00:ad:b1)		
	LAN	em1 (00:0c:29:00:ad:bb)		
	WAN2	em2 (00:0c:29:00:ad:c5)		
	SYNC	em3 (00:0c:29:00:ad:cf)		
	Interfaces that are configured as	members of a lagg(4) interface will not be shown.		

Luego asignamos la IP correspondiente a cada interfaz desde Interfaces  $\rightarrow$  [Placa Correspondiente]



Asignamos la IP a la interfaz de sincronización:

*Sense	System Interfaces	Firewall      Services      VPN      Status      Diagnostics      Help      Grageronet-f									
	General configuration										
	Enable	Enable Interface									
	Description	SYNC Enter a description (name) for the interface here.									
	Туре	Static 💌									
	MAC address	Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx									
	MTU	N If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.									
	MSS	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.									
	Speed and duplex	Advanced - Show advanced option									
	Static IP configuration										
	IP address	▶ 1.1.1.1									
	Gateway	None 💌 -or- add a new one. If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above									
	Private networks										

Luego a la placa de LAN:

4

Sense ,	► System ► Interfaces	→ Firewall → Services → VPN → Status → Diagnostics → Help 🔒 gen	ronet-										
	Interfaces: LAN	6	0										
	General configuration												
	Enable	Enable Interface											
	Description	LAN Enter a description (name) for the interface here.											
	Туре	Static 💌											
	MAC address	MAC address Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx											
	MTU If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.												
	MSS	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.											
	Speed and duplex	Advanced - Show advanced option											
	Static IP configuration												
	IP address	192.168.2.1 / 24 💌											
	Gateway	None 💌 -or- add a new one. If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above											

Y por último a la placa WAN, a la cual ademas le asignamos el gateway correspondiente proporcionado por el ISP:

<b>Sense</b>	<ul> <li>System</li> </ul>	<ul> <li>Interfaces</li> </ul>	▶ Firewall	<ul> <li>Services</li> </ul>	► VPN	<ul> <li>Status</li> </ul>	<ul> <li>Diagnostics</li> </ul>	<ul> <li>Help</li> </ul>	밝• geronet-fi			
	Interface	es: WAN1							6 0			
	General co	onfiguration										
	Enable		🗹 Enable I	nterface 🔶								
	Description		📏 WAN1 Enter a descri	ption (name) for th	e interface here.							
	Туре		Static 💌									
	MAC addres	55	Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx									
	MTU		If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.									
	MSS		If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.									
	Speed and	duplex	Advanced	- Show advanced	option							
	Static IP o	configuration										
	IP address		<b>N</b> 10.0.1.2	2	/ 24 💌 🤙							
	Gateway		WAN1GW - 10 If this interface	0.1.1 💌 -or- add a r is an Internet connect	new one. ion, select an existin	q Gateway from the list	or add one using the li	ink above				

Ahora se deben asignar las IPs Virtuales que hemos definido. Vamos a Firewall  $\rightarrow$  Visrtual IPs

<b>Sense</b>	<ul> <li>System</li> <li>Interfaces</li> </ul>	✓ Firewall →	Services	•	VPN
		Aliases			
		NAT			
	Interfaces: WAN1	Rules			
		Schedules			
		Traffic Shaper			
	General configuration	Virtual IPs 🔶			
	Enable	Enable Interfa	ce		

En la pestaña Virtual IPs debemos pulsar en el botón (+) para agregar una nueva VHID.

<b>Sense</b>	► System ► Interfaces ► Firewall	<ul> <li>Services</li> </ul>	► VPN	<ul> <li>Status</li> </ul>	Diagnostics	Help 😫 g	eronet-fi
	Firewall: Virtual IP Address	ses					0
	Virtual IPs						_
	Virtual IP address	Туре	Description			3	
	10.0.1.250/24 (vhid 1)		CARP WAN1				
	10.0.2.250/24 (vhid 2)		CARP WAN2			e 🗴	
	192.168.2.250/24 (vhid 3)		CARP LAN			e 🗴	
	Note: The virtual IP addresses defined on this page m You can check the status of your CARP Virtual I	ay be used in NAT i Ps and interfaces he	mappings. ere.				

Primero agregamos la IP virtual de la WAN. Es importante que se seleccione el Type CARP.

En el campo Virtual IP Password debemos settear una clave que se insertará igual en ambos firewall.

Y ademas el VHID Group debe configurarse de la misma forma en ambos firewalls.

Edit Virtual TD	
Туре	Proxy ARP      CARP
Interface	WAN1
IP Address(es)	Type:       Network         Address:       10.0.1.250         Address:       10.0.1.250         range.       Expansion:         Expansion:       Disable expansion of this entry into IPs on NAT lists (e.g. 192.168.1.0/24 expands to 256 entries.)
Virtual IP Password	Enter the VHID group password.
VHID Group	1 VHID group that the machines will share
Advertising Frequence	y         Base: 1 Skew: 0            The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.
Description	CARP WAN1 You may enter a description here for your reference (not parsed).
	Save

Luego configuramos el VHID de la red LAN de la misma forma en ambos dispositivos.

Edit Virtual IP	
Туре	Proxy ARP     CARP
Interface	
IP Address(es)	Type:       Network         Address:       192.168.2.250         Address:       192.168.2.250         range.       Expansion:         Expansion:       Disable expansion of this entry into IPs on NAT lists (e.g. 192.168.1.0/24 expands to 256 entries.)
Virtual IP Password	Enter the VHID group password.
VHID Group	3  The Enter the VHID group that the machines will share
Advertising Frequency	Base: 1 V Skew: 0 V
	The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of bo values in the cluster determines the master.

Note: Proxy ARP and Other type Virtual IPs cannot be bound to by anything running on the firewall, such as IPsec, OpenVPN, etc. Use a CARP or IP Alias type address for these cases.

For more information on CARP and the above values, visit the OpenBSD CARP FAO.

#### El siguiente paso solo debemos hacerlo en el firewall principal:

En la pestaña **CARP Settings** debemos tildar la opción Synchronize States, seleccionamos la interfaz definida para tal caso (SYNC) y seteamos la IP del otro firewall (en el ejemplo la IP de sincronización del firewall 2 de backup) con la cual se replicará el estado.

<b>Sense</b>	<ul> <li>System</li> </ul>	<ul> <li>Interfaces</li> </ul>	<ul> <li>Firewall</li> </ul>	<ul> <li>Services</li> </ul>	► VPN	•	Status	Diagnostics	•	Help	음 <mark>॰ geronet-</mark> fi	
	Services	CARP Settings	tings: Edi	t							0	
	State Sync	hronization Setti	ngs (pfsync)									
	Synchronize	States	pfsync transfers via multicast on similar message This setting sho NOTE: Clicking	state insertion, u a specified interfa s from other firew uld be enabled on save will force a c	pdate, and dele ice, using the P alls, and import all members of onfiguration syr	ion messa SYNC prot s them into a failover c if it is en	ges between cocol (IP Prot o the local sta group. abled! (see C	firewalls. Each firewa ocol 240). It also liste ite table. onfiguration Synchroi	Il sends ins on th nization !	these mess at interface Settings bel	ages out e for low)	
	Synchronize Interface SYNC Synchronize States is enabled, it will utilize this interface for communication. NOTE: We recommend setting this to a interface other than LAN! A dedicated interface works the best. NOTE: You must define a IP on each machine participating in this failover group. NOTE: You must have an IP assigned to the interface on any participating sync modes.											
	pfsync Syncl	hronize Peer IP	N 1.1.1.2 Setting this opt	ion will force pfsyn	c to synchroniz	e its state t	able to this I	P address. The defau	lt is direc	cted multica	əst.	
	Configurat	ion Synchronizati	ion Settings (XI	1LRPC Sync)								
	Synchronize	Config to IP	NOTE: Do not	dress of the firewa sync is currently o system's port and <b>use the Synchro</b>	Il to which the sonly supported of protocol are s	elected convertion of the conv	nfiguration sections using t gly!	ections should be syn he same protocol and <b>tion on backup clus</b>	chronize I port as <b>ter me</b> r	d. this system m <b>bers!</b>	n - make	

Mas abajo debemos establecer el usuario y clave de administración del dispositivo de backup y sellecionar las características que se desean sincronizar:







Pulsando en Save guardaremos los cambios.

El siguiente paso consiste en habilitar en ambos firewalls una regla que permita la comunicación

entre las placas de sincronización de ambos dispositivos.

## Para ello vamos a Firewall $\rightarrow$ Rules $\rightarrow$ Placa SYNC



En nuestro caso habilitamos el tráfico completo en dicha interfaz:

<b>Sense</b>	<ul> <li>Systematic</li> </ul>	em	► Interfa	aces 🕨 🕨	Firewall	<ul> <li>Services</li> </ul>	•	VPN •	Status	► Diagno	ostics 🔸 H	Help 🚽 🛱 gerone
	Firew	vall:		WANZ	SYNC		_					600
	Tiodun	ID	Proto	Source	Port	Destination	Port	Gateway	Oueue	Schedule	Description	8P
			TCP/UDP	*	*	*	*	*	none		Permitir SYN	
	_											
	pasi pasi	s s (disab	oled)		🔀 blo	ck (disabled)			reject reject (disa	abled)		<ul> <li>log</li> <li>log (disabled)</li> </ul>
	Hint:								1		11	
		Rules block	are evaluate rules, you'll l	d on a first- have to pay	match basis (i. attention to th	e. the action of ti e rule order. Eve	ne first rul rything tha	e to match a pao t isn't explicitly	cket will be e passed is blo	executed). This acked by default	t.	u use

Una vez aplicada la regla en ambos equipos, podremos comprobar el status del Cluster de firewall llendo a Status  $\rightarrow$  CARP (failover)

Sense /	<ul> <li>System</li> </ul>	m	<ul> <li>Interfa</li> </ul>	aces I	<ul> <li>Firewall</li> </ul>	<ul> <li>Services</li> </ul>	•	VPN	<ul> <li>Status</li> </ul>	► Di	iagnos	stics
	Firew	all:	Rules						CARP (failover) Dashboard DHCP Leases			
	Floating	) w	AN1 LAN	WAN2	SYNC				Gateways Interfaces			
		ID	Proto	Source	Port	Destination	Port	Gateway	IPsec	Sched	ule	Desc
			TCP/UDP	*	*	*	*	*	Load Balancer OpenVPN			Perm
									Package Logs Queues			
	■ pass pass (disabled)     Solution     disabled)     Solution     disabled     Solution     disabled     Solution     disabled     Solution     disabled     Solution     Solutio								Services System Logs	led)		
	Hint:	Rules	are evaluate	ed on a firs	t-match basis	(i.e. the action of t	he first ru	le to match a	Traffic Graph UPnP & NAT-P	MP.	. This r	neans t

Si estamos situados en el firewall principal veremos que el status de las Virtuals IPs es MASTER y con la flecha verde nos indica que está online:

Sense /	▶ System	► Interfaces	▶ Firewall	► Server	ices 🕨 🕨	VPN	×	Status	<ul> <li>Diagnostics</li> </ul>	×	Help	음• geronet-fi
	Status: C	ARP										0
	1000	CARP Inte	rface			Virtua	IP			Sta	tus	
1.000		vip1						🗅 м				
and the second second		vip2						🗅 м				
		vip3				192.168	.2.250			🕨 М	ASTER	
	Note: You can configu pfSync nodes: 6814c4c5 804a2b1a aa72e4d3	re CARP settings h	ere.									

Si nos logueamos en el firewall de backup veremos que el status de las Virtuals IPs dice Backup

🧲 🕘 🤫 ht	tp:// <b>192.168.2.2</b> /		۶	v-⊠c×	🈵 gerone	et-firewall2.	geronet.c ×				
<u>A</u> rchivo <u>E</u> dició	in <u>V</u> er <u>F</u> avoritos	<u>H</u> erramientas	A <u>y</u> uda								
👍 🍅 Dexter ve	r online - descar 🚺	YouTube - Bro	adcast You	. 👌 Google	Académico	W Wonde	rware Home	🌀 Faculty Co	ontact (	Center - S	G Correo
<b>Sense</b>	▶ System ▶ I	nterfaces 🔹 🕨	Firewall	<ul> <li>Services</li> </ul>	► VP	N 🕨	Status	Diagnostics	•	Help	음• geror
	Status: Dash	nboard									?
	System Information			E		Interfaces					
	Name	geronet-firewall	2.geronet.com	n.ar		MAN1	L	10.0.1.3	1000ba	seT <full-dup< th=""><th>lex&gt;</th></full-dup<>	lex>
	Version	2.0.1-RELEAS	E (i386) c 12 18·24·17	7 EST 2011				192.168	.2.2 100	)0baseT <full-< th=""><th>duplex&gt;</th></full-<>	duplex>
		FreeBSD 8.1-RELEASE-p6		257 2011			2	10.0.2.3	1000ba	seT <full-dup< td=""><td>lex&gt;</td></full-dup<>	lex>
		Unable to check	for updates.			SYNC		1.1.1.2	1000bas	eT <full-duple< td=""><td>ex&gt;</td></full-duple<>	ex>
and the second sec	Platform	ofSense									

*Sense	<ul> <li>System</li> </ul>	▶ Interfaces	► Firewall	<ul> <li>Services</li> </ul>	► \	/PN	<ul> <li>Status</li> </ul>	<ul> <li>Diagnostics</li> </ul>	<ul> <li>Help</li> </ul>	片 geronet-f	
	Status: C	ARP								0	
	CARP Interface					Virtual I	Р		Status		
1000	vip1 vip2				10.0.1.250 10.0.2.250				BACKUP		
and the second second									BACKUP		
and the second		vip3				192.168.2.	250		BACKUP		
	Note: You can configur pfSync nodes: 48f8288e 86b31a37 ad8305b2 c323c81f	e CARP settings h	ere.								

Por último, si queremos verificar que la sincronización está funcionando correctamente podemos probarlo aplicando una regla de firewall en uno de los dispositivos y luego verificando que en el otro se a replicado automáticamente.