

Diseño general de alta disponibilidad WAN en pfSense

Índice

1. Escenario.....	3
2. Configuración.....	3
2.1. Interfaces.....	3
2.2. Gateway.....	4
2.3. Firewall.....	6
3. Comprobaciones.....	7

1.Escenario.

Para el escenario he usado VirtualBox y he creado tres máquinas virtuales, una de ellas es un cortafuegos PfSense, al cual le he configurado 3 tarjetas de red, una WAN con la red 10.0.2.0/24, otra WAN con la red 10.0.3.0/24 y otra con la red interna de PfSense con la 192.168.1.0/24; he creado una máquina virtual con Ubuntu la cual hará de estudiante en una clase de informática y se situará en la red interna, también se ha creado otra máquina Ubuntu que actuará de servidor externo como podría ser cualquier página web y se sitúa de una WAN, tiene instalado apache por el simple hecho de hacer pruebas.

2.Configuración.

2.1. Interfaces

Comenzando la configuración lo primero que debemos hacer es asignar a cada una de las interfaces una conexión, Para ello vamos a Interfaces à assign y configuramos la conexiones WAN1, WAN2 y LAN. Es decir definimos que placa se va a conectar a qué servicio:

Una vez hecho esto debemos de asignar a cada interfaz una dirección IP:

WAN2 Interface (opt1, em2)	
Status	up
DHCP	up Release WAN2 <input type="checkbox"/> Relinquish Lease
MAC Address	08:00:27:2f:4a:84
IPv4 Address	10.0.3.4
Subnet mask IPv4	255.255.255.0
Gateway IPv4	10.0.3.1
IPv6 Link Local	fe80::a00:27ff:fe2f:4a84%em2
DNS servers	212.166.132.116 212.166.132.104
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	2891/2914 (86 KiB/86 KiB)
In/out packets (pass)	2891/2914 (86 KiB/86 KiB)
In/out packets (block)	0/0 (0 B/0 B)
In/out errors	0/0
Collisions	0
Interrupts	4163 (3/s)

2.2. Gateway

Para que los alumnos puedan tener salida a internet se le debe de configurar un gateway a cada interfaz WAN que hayamos creado, para ello vamos a System > Routing y ahí agregamos nuestras interfaces:

Edit Gateway

Disabled

☐ Disable this gateway

Set this option to disable this gateway without removing it from the list.

Interface

WAN

Choose which interface this gateway applies to.

Address Family

IPv4

Choose the Internet Protocol this gateway uses.

Name

WAN_DHCP

Gateway name

Gateway

dynamic

Gateway IP address

Gateway Monitoring

☐ Disable Gateway Monitoring

This will consider this gateway as always being up.

Gateway Action

☐ Disable Gateway Monitoring Action

No action will be taken on gateway events. The gateway is always considered up.

Monitor IP

Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).

Static route

☐ Do not add static route for gateway monitor IP address via the chosen interface

By default the firewall adds static routes for gateway monitor IP addresses to ensure traffic to the monitor IP address leaves via the correct interface. Enabling this checkbox overrides that behavior.

Force state

☐ Mark Gateway as Down

This will force this gateway to be considered down.

State Killing on Gateway Failure

Use global behavior (default)

Controls the state killing behavior when this specific gateway goes down. Killing states for specific down gateways only affects states created by policy routing rules and reply-to. Has no effect if gateway monitoring or its action are disabled or if the gateway is forced down. May not have any effect on dynamic gateways during a link loss event.

Edit Gateway

Disabled

☐ Disable this gateway

Set this option to disable this gateway without removing it from the list.

Interface

WAN2

Choose which interface this gateway applies to.

Address Family

IPv4

Choose the Internet Protocol this gateway uses.

Name

WAN2_DHCP

Gateway name

Gateway

dynamic

Gateway IP address

Gateway Monitoring

☐ Disable Gateway Monitoring

This will consider this gateway as always being up.

Gateway Action

☐ Disable Gateway Monitoring Action

No action will be taken on gateway events. The gateway is always considered up.

Monitor IP

Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).

Static route

☐ Do not add static route for gateway monitor IP address via the chosen interface

By default the firewall adds static routes for gateway monitor IP addresses to ensure traffic to the monitor IP address leaves via the correct interface. Enabling this checkbox overrides that behavior.

Force state













☐ Mark Gateway as Down

This will force this gateway to be considered down.

State Killing on Gateway Failure

Use global behavior (default)

Controls the state killing behavior when this specific gateway goes down. Killing states for specific down gateways only affects states created by policy routing rules and reply-to. Has no effect if gateway monitoring or its action are disabled or if the gateway is forced down. May not have any effect on dynamic gateways during a link loss event.

Gateways							
	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
	<input checked="" type="checkbox"/> WAN_DHCP 		WAN	10.0.2.1	10.0.2.1	Interface WAN_DHCP Gateway	   
	<input checked="" type="checkbox"/> WAN_DHCP6		WAN			Interface WAN_DHCP6 Gateway	 
	<input checked="" type="checkbox"/> WAN2_DHCP		WAN2	10.0.3.1	10.0.3.1	Interface WAN2_DHCP Gateway	 
	<input checked="" type="checkbox"/> WAN2_DHCP6		WAN2			Interface WAN2_DHCP6 Gateway	 

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 > Gateway > Groups:

System / Routing / Gateway Groups

Gateways

Static Routes

Gateway Groups

Gateway Groups

Group Name	Gateways	Priority	Description	Actions
WANGROUP	WAN_DHCP WAN2_DHCP	Tier 1 Tier 2		<div><div></div><div></div><div></div></div>

+

Add

Ahora bien, llegados a este punto debemos de configurar el grupo de gateway, debemos de asignar a cada gateway un tier, esto nos servirá para darle prioridad a cierto gateway y de esta manera permitir que la red se regule en caso de un exceso de carga:

Edit Gateway Group Entry				
Group Name	<input type="text" value="WANGROUP"/>			
Gateway Priority				
	<input type="text" value="WAN_DHCP"/>	<input type="text" value="Tier 1"/>	<input type="text" value="Interface Address"/>	<input type="text" value="Interface WAN_DHCP Gateway"/>
	<input type="text" value="WAN2_DHCP"/>	<input type="text" value="Tier 2"/>	<input type="text" value="Interface Address"/>	<input type="text" value="Interface WAN2_DHCP Gateway"/>
	Gateway	Tier	Virtual IP	Description
Link Priority	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 then the next available link(s) in the next priority level will be used.			
Virtual IP	The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.			
Trigger Level	<input type="text" value="High Latency"/> When to trigger exclusion of a member			
Description	<input type="text"/> A description may be entered here for administrative reference (not parsed).			

Una vez hecho esto podemos continuar a agregar una regla para el firewall.

2.3. Firewall

Debemos de configurar una regla para la LAN que haga que todos los paquetes provenientes de la LAN circulen por el WANGROUP que acabamos de crear, para ello nos disponemos a Firewall > Rules y creamos la siguiente regla:

Edit Firewall Rule			
Action	<div>Pass</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</div>		
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	<div>LAN</div> <div>Choose the interface from which packets must come to match this rule.</div>		
Address Family	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>		
Protocol	<div>Any</div> <div>Choose which IP protocol this rule should match.</div>		
Source			
Source	<input type="checkbox"/> Invert match	<div>Any</div>	<div>Source Address</div> / <div></div>
Destination			
Destination	<input type="checkbox"/> Invert match	<div>Any</div>	<div>Destination Address</div> / <div></div>
Gateway	<div>WANGROUP</div> <div>Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing. Gateway selection is not valid for "IPv4+IPv6" address family.</div>		

De esta manera los alumnos ya podrán tener acceso a internet.

3.Comprobaciones.

A continuación muestro una serie de capturas del Status tanto de las interfaces como de los gateway:

WAN Interface (wan, em0)

Status

up

↑

DHCP

up

Release WAN

☐ Relinquish Lease

MAC Address

08:00:27:ac:67:01

IPv4 Address

10.0.2.4

Subnet mask IPv4

255.255.255.0

Gateway IPv4

10.0.2.1

IPv6 Link Local

fe80::a00:27ff:feac:6701%em0

DNS servers

212.166.132.116

212.166.132.104

MTU

1500

Media

1000baseT <full-duplex>

In/out packets

10232/9110 (4.59 MiB/524 KiB)

In/out packets (pass)

10232/9110 (4.59 MiB/524 KiB)

In/out packets (block)

0/0 (0 B/0 B)

In/out errors

0/0

Collisions

0

Interrupts

11295 (4/s)

LAN Interface (lan, em1)

Status

up

↑

MAC Address

08:00:27:92:3c:d0

IPv4 Address

192.168.1.1

Subnet mask IPv4

255.255.255.0

IPv6 Link Local

fe80::a00:27ff:fe92:3cd0%em1

MTU

1500

Media

1000baseT <full-duplex>

In/out packets

12421/13019 (1.17 MiB/6.94 MiB)

In/out packets (pass)

12421/13019 (1.17 MiB/6.94 MiB)

In/out packets (block)

10/0 (616 B/0 B)

In/out errors

0/0

Collisions

0

Interrupts

16172 (6/s)

WAN2 Interface (opt1, em2)

Status

up

↑

DHCP

up

Release WAN2

☐ Relinquish Lease

MAC Address

08:00:27:2f:4a:84

IPv4 Address

10.0.3.4

Subnet mask IPv4

255.255.255.0

Gateway IPv4

10.0.3.1

IPv6 Link Local

fe80::a00:27ff:fe2f:4a84%em2

DNS servers

212.166.132.116

212.166.132.104

MTU

1500

Media

1000baseT <full-duplex>

In/out packets

4979/5012 (147 KiB/147 KiB)

In/out packets (pass)

4979/5012 (147 KiB/147 KiB)

In/out packets (block)

0/0 (0 B/0 B)

In/out errors

0/0

Collisions

0

Interrupts

7106 (3/s)

Gateways

Name	Gateway	Monitor	RTT	RTTsd	Loss	Status	Description	Action
WAN_DHCP (default)	10.0.2.1	10.0.2.1	1.351ms	0.6ms	0.0%	Online	Interface WAN_DHCP Gateway	<div>⌵⌵⌵</div>
WAN_DHCP6			Pending	Pending	Pending	Pending	Interface WAN_DHCP6 Gateway	<div>⌵</div>
WAN2_DHCP	10.0.3.1	10.0.3.1	1.109ms	0.454ms	0.0%	Online	Interface WAN2_DHCP Gateway	<div>⌵⌵</div>
WAN2_DHCP6			Pending	Pending	Pending	Pending	Interface WAN2_DHCP6 Gateway	<div>⌵</div>

Gateway Groups

Group Name	Gateways	Description	Action
WANGROUP	<div><div>Tier 1</div><div><div>WAN_DHCP</div><div>Online</div></div></div> <div><div>Tier 2</div><div><div>WAN2_DHCP</div><div>Online</div></div></div>		<div>⌵</div>

Y aquí podemos ver la página del servidor externo:

