

Alta disponibilidad con PfSense.

Índice

1. Escenario.	3
2. Configuración.	3
2.1. Interfaces.	3
2.2. Modo CARP.	4
2.3. Reglas.	5
3. Comprobaciones.	5

1. Escenario.

En este escenario tenemos dos máquinas virtuales con PfSense, ambas máquinas cuentan con 4 interfaces de red, una de ella es la WAN1 la otra es la WAN2 la otra es la LAN y por último es la SYNC que sirve para sincronizar ambos PfSense.

Contamos con una máquina virtual con Ubuntu que se encontrará en la LAN.

2. Configuración.

2.1. Interfaces.

Para las interfaces hemos añadido simplemente una interfaz más a las interfaces que ya teníamos en el diseño de PfSense, debemos de añadir una interfaz de sincronización para la transmisión de información entre ambos PfSense, para ello vamos a asignar la interfaz a la tarjeta de red:







SYNC

em3 (08:00:27:42:12:fb)

Delete

En el caso de PfSense Master la ip es 1.1.1.1 y en el caso del Slave es 1.1.1.2.

También debemos de añadir 3 interfaces virtuales, una para la WAN1, para la WAN2 y para la LAN:

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
10.0.2.250/24 (vhid: 1)	WAN	CARP		 
10.0.3.250/24 (vhid: 2)	WAN2	CARP		 
192.168.1.250/24 (vhid: 3)	LAN	CARP		 

Dichas interfaces han de ser iguales y con las mismas IPs en ambos PfSense.

Al tener dichas IP activas digamos que ya podemos empezar a configurar el modo CARP, que sirve para compartir una serie de IP predeterminadas.

2.2. Modo CARP.

El modo CARP nos permite “enlazar” ambos PfSense y de esta manera permite sincronizar los cambios en ambos PfSense.

Debemos situarnos en la sección de System > High Availability:

State Synchronization Settings (pfsync)

Synchronize states

☒ pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface

SYNC

If Synchronize States is enabled this interface will be used for communication.
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
An IP must be defined on each machine participating in this failover group.
An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID

0ae1af63

Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.
Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).
Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer IP

1.1.1.2

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

1.1.1.2

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username

admin

Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password

Enter the webConfigurator password of the system entered above for synchronizing the configuration.

Confirm

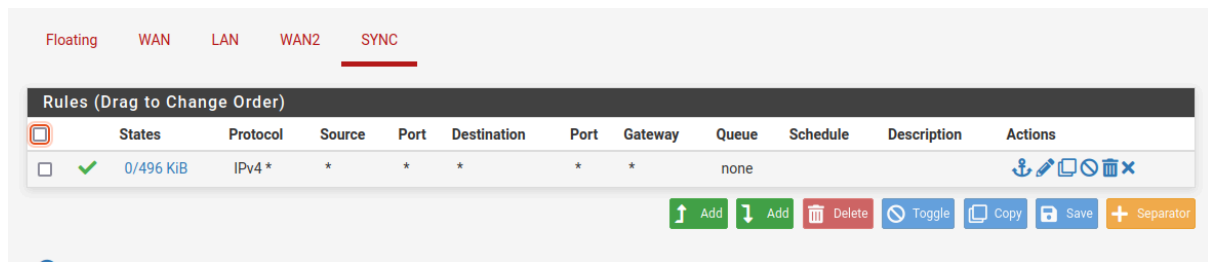
Aquí debemos de poner la IP del PfSense esclavo (esta configuración solo se hace en el PfSense Master) para su sincronización, al igual que el nombre y la contraseña del usuario PfSense Slave, en mi caso es Admin, también debemos de seleccionar qué cosas se van a sincronizar:

Select options to sync

☒ User manager users and groups
☒ Authentication servers (e.g. LDAP, RADIUS)
☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
☒ Firewall rules
☒ Firewall schedules
☒ Firewall aliases
☒ NAT configuration
☒ IPsec configuration
☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)
☒ DHCP Server settings
☒ DHCP Relay settings
☒ DHCPv6 Relay settings
☒ WoL Server settings
☒ Static Route configuration
☒ Virtual IPs
☐ Traffic Shaper configuration
☐ Traffic Shaper Limiters configuration
☒ DNS Forwarder and DNS Resolver configurations
☐ Captive Portal
☒ Toggle All

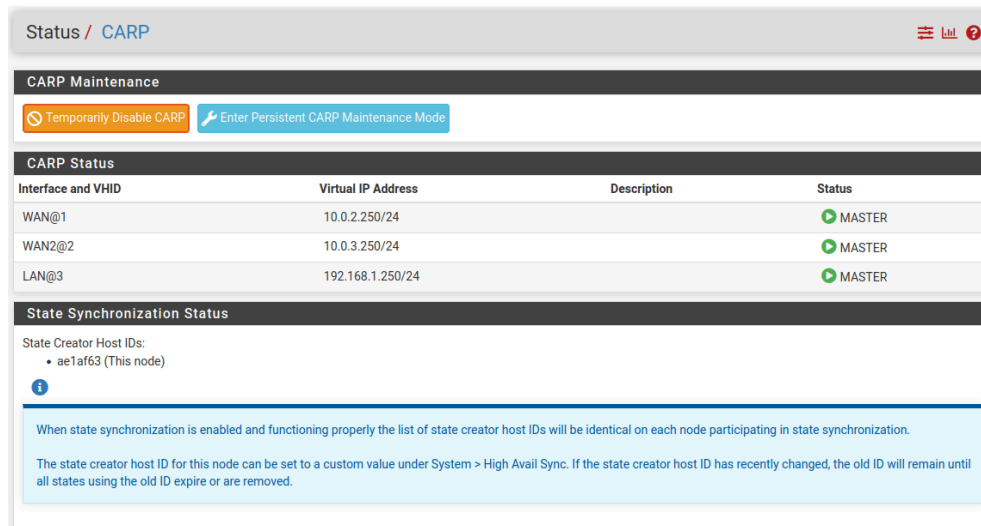
2.3. Reglas.

Para que ambos cortafuegos tengan contacto entre ellos debemos de añadir una regla para la interfaz SYNC que permite todo el tráfico:

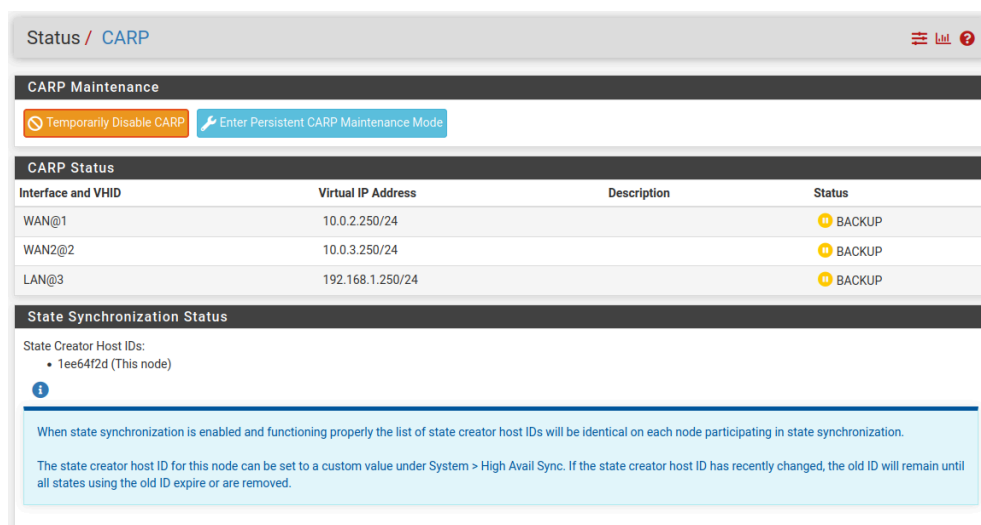


3. Comprobaciones.

Para las comprobaciones podemos ir a la sección de Status > CARP y veremos lo siguiente:



Eso en el Master.



Y esto en el Slave.

Otra manera de comprobar que funciona bien es añadir una regla al cortafuegos Master y ver que se crea en el Slave:

Marcos Cáceres García

▀ ubuntu [Corriendo] - Oracle VM VirtualBox 2024-04-25 14-17-15.mp4