Virtual MAC Addresses

https://campus.barracuda.com/doc/98213637/

The availability of an HA-pair of CloudGen firewalls can be affected in networks where switches block ARP packets or where industrial TCP/IP stacks can not send ARP packets for service IP addresses. In order to be able to operate HA firewalls in such critical infrastructures, the application of virtual MAC addresses on an HA-pair of CloudGen firewalls now improves the overall availability.

The concept of a virtual MAC address provides a way of assigning virtual ethernet addresses to a certain interface. Although the requirement to use virtual MAC addresses is not always necessary, there are still certain situations where using them is important. A concrete and practically relevant example is the option to use virtual MAC addresses to improve the HA availability of the CloudGen firewall.

Virtual MAC addresses cannot be configured for non-HA firewalls.

Using Virtual MAC Addresses on an ESXi Hypervisor

If you want to use a MAC address in an ESXi hypervisor, you must accept the following security options in the related configuration section on your ESXi hypervisor.

Security	Configuration Setting
Promiscuous mode	Accept
MAC Address Changes	Accept
Forged Transmits	Accept

As a general recommendation, ensure that the settings on the hypervisor of your provider allow you to change the MAC addresses.

For more information, see your manuals for your ESXi hypervisor.

Using Virtual MAC Addresses for HA

An HA cluster depends on clients accepting gratuitous and/or unsolicited ARP packets sent for service IP addresses. However, if switches block these ARP packets or if certain clients operate some industrial TCP/IP stacks where processing ARP packets is not implemented, the HA concept can not act out its full potential.

As of firmware 9.0.0, and in order to circumvent these limitations, the CloudGen firewall supports the

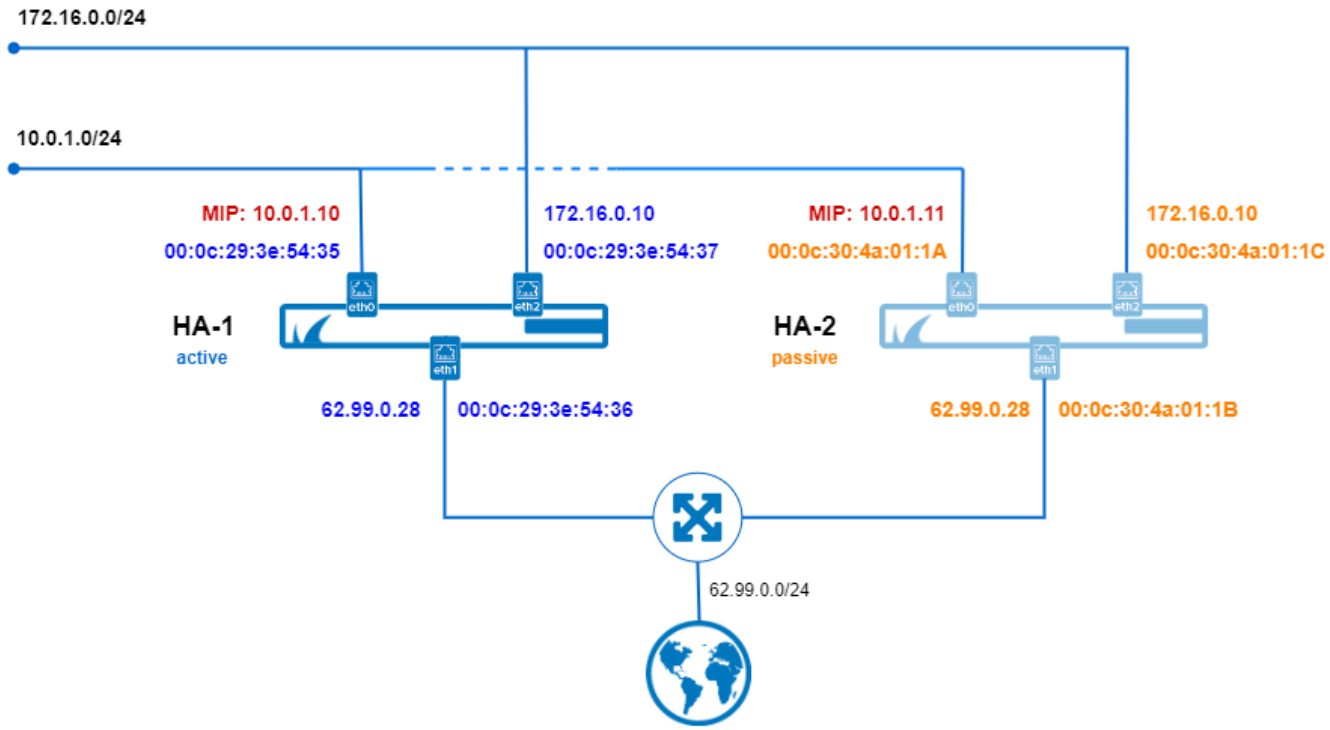
usage of virtual MAC addresses when operating an HA pair of CGF firewalls. Practically, when an HA failover is executed, the active firewall swaps its MAC addresses and its assigned shared IP addresses with the passive firewall which is going to be the active firewall after the failover. Because the clients also know the MAC addresses from the firewall they were communicating to before the failover, the clients will find the same MAC addresses with their associated shared IP addresses and thus reconnect seamlessly to the other HA partner after the failover.

Important Note

MAC addresses are always swapped when there are shared IPs on a configured network. This applies to all configured networks on all interfaces, especially to the network the MIP is located in.

This example also assumes that there are shared IPs configured in the MIP network!

The following image shows the MAC and IP addresses of an HA pair of CG firewalls before an HA failover. Note that the illustrations do not contain shared IP addresses that are required to be configured in the MIP network for the MAC address to be swapped!

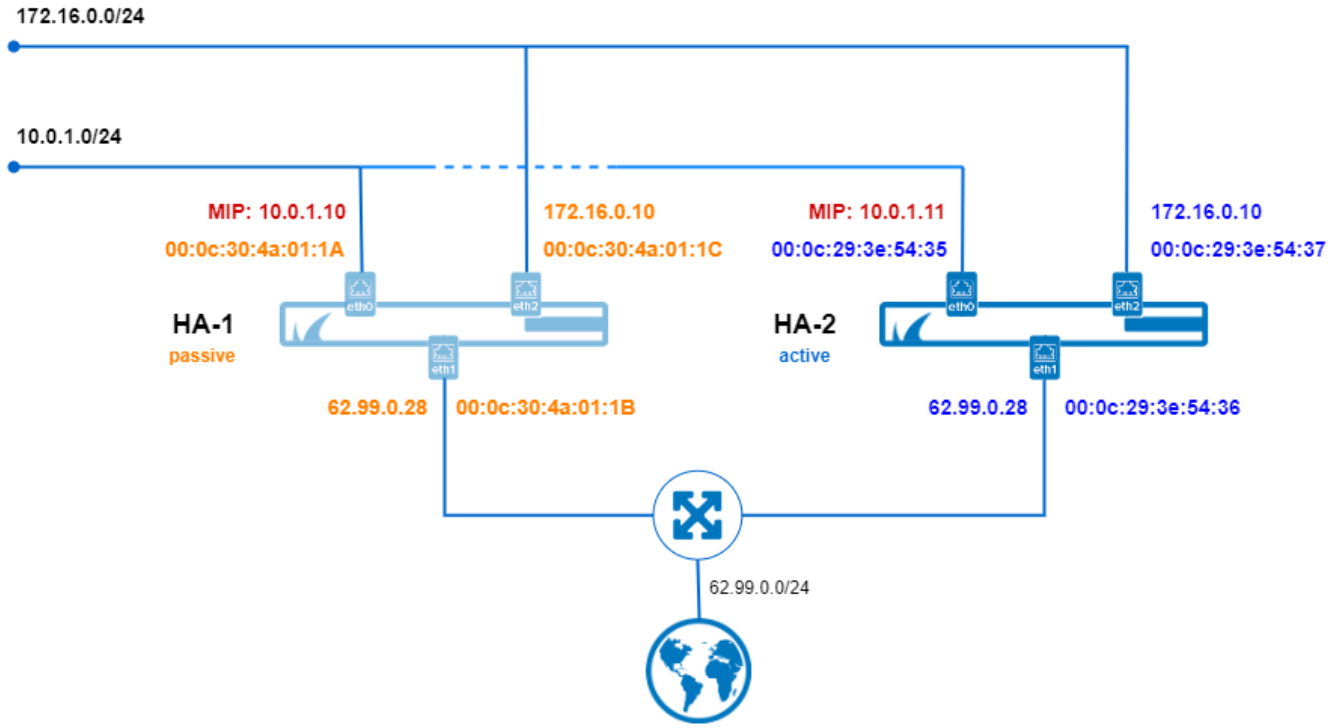


VLANs and Ethernet Bundles are in the same way fully supported as virtual routers.

Besides this, the MAC addresses of the related management IP addresses are also swapped. However,

the original management IP addresses remain untouched on each of the two HA firewalls in order to access the primary and the secondary firewall independently under their original IP addresses.

The following image shows the MAC and IP addresses of an HA pair of CG firewalls after an HA failover.



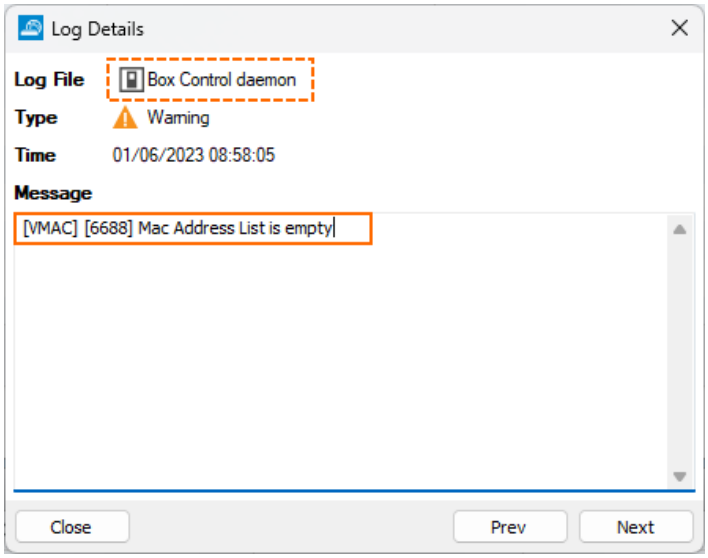
For the clients, the usage of virtual MAC addresses makes gratuitous and/or unsolicited ARPs for service IPs obsolete and improves the overall high availability experience.

This handling of virtual MAC addresses in the context of high availability is fully transparent to the user and requires no manual configuration. In fact, the only thing to do is to activate the usage of virtual MAC addresses. After the activation, the affected firewalls will manage to take care of all necessary measures as described above.

Logging

If you experience problems with virtual MAC addresses, it is recommended to increase the logging level to get more detailed feedback. Related logging entries are stored in the `box_control_deamon` log.

You can identify the logged entries created by the Box Control Daemon on their prefix '[VMAC]'.


Log Details
Log File
Box Control daemon
Type
Warning
Time
01/06/2023 08:58:05
Message
[VMAC] [6688] Mac Address List is empty
Close
Prev
Next

Figures

1. vMAC_nw_layout_before_HA_failover.png
2. vMAC_nw_layout_after_HA_failover.png
3. vMAC_log_details.png