High Availability in opnSense

This is just notes on how we built one. Both of our routers are virtuals, running under the KVM hypervisor. That allowed a bunch of shortcuts, such as defining vlans at the hypervisor levels and replicating a running router for the second one. We used two separate machines; the hypervisor was mainly so we could put some additional low resource virtuals on the same physical machine.

We'll need one share IP for each interface, so one IP for each router, and one shared one, so a total of 3 IP's set aside for the set.

Initial

1. Define network bridges to be used by the router, one per vlan to be used
2. Create one router (hint, tell the hypervisor to use the FreeBSD predefined)
    1. Don't need much disk space; 10G appears to be just fine
    2. In our machine, we did not have AES, so we increased processors to 4 and RAM to 8G
3. Do standard install, defining the network interfaces, etc...
4. Shut down virtual (router)
5. replicate configuration and storage to second machine
    1. Reconfigure name
    2. Reconfigure MAC addresses for virtual
6. Bring up second machine (first one still down). Connect and change name and IP's on all interfaces
7. Bring up first machine

You should now have two virtually identical installations, with only the name, IP's and MAC addresses different.

Configure HA

I did NOT set up as recommended with an additional interface only for CARP. Instead, I used the LAN interface for that.

1. Verify LAN interface accepts CARP. By default, it is set to accept all traffic from the LAN, but make sure this is the case (see Firewall | Rules | LAN)
2. On the primary router
    1. Interfaces | Virtual IPs | Settings
        1. Add
        2. Mode: CARP
        3. Interface: Choose one of the interfaces
        4. Address: the shared IP address for that interface
        5. Virtual IP Password: Choose a random password
        6. VHID Group: push button for Select and unassigned VHID
        7. Advertising Frequency:
            1. Base: 1

        2. Skew: 0
    8. Description: make it simple. I use VIP “interface name”, ie VIP WAN or VIP LAN. The VIP is for Virtual IP.
    9. Save
    10. Repeat for all other interfaces (hint, you can clone an interface, then change the Interface, Address, VHID Group and Description).
2. For each subnet which will be routing through the firewall, do the following. For example, if you have a subnet that only provides resources for other subnets, don't do this. But, for LAN, or anything else that will directly access the 'net. **You are setting outbound to use the CARP interface**:
    1. Firewall | NAT | outbound
    2. Change existing rules to use the CARP IP
    3. Create new rules for any other subnets (hint, clone the LAN, then make the changes needed)

Additional

1. Change DHCP server to set the gateway to the Virtual IP
2. Change DHCP server to set DNS to correct value (if not using defaults)

Set up sync

1. On master router
    1. System | High Availability | Settings
        1. Synchronize States: check
        2. Synchronize Interface: The interface it will communicate on
        3. Synchronize Peer IP: the IP address of the backup router
        4. Synchronize Conifig to IP: The same IP (IP of the backup router)
        5. Remote System Username: A user on the backup router with full admin privileges
        6. Remote System Password: Password for that user
        7. Put a check mark in every system you want sync'd. At the very least, you need
            1. Users and Groups
            2. Certificates
            3. Firewall Rules
            4. Firewall Schedules
            5. Firewall Categories
            6. Aliases
            7. NAT
            8. DHCPD (well, I want them sync'd)
            9. Virtual IP's (you MUST have this)
            10. Static Router
            11. OpenVPN, if you're going to use that
            12. Firewall Groups
            13. Unbound DNS (again, I want that)
        8. Click Save
2. On backup Router
    1. System | High Availability | Settings
        1. Synchronize States: Check

        2. Interface: Select correct interface
        3. Synchronize Peer IP: IP of Master router
        4. Save (Do **not** put any additional information in)
    3. Reboot both firewalls if you want. Sometimes avoids problems
    4. On master router
        1. System | High Availability | Status
        2. Click the little round thing at the bottom, where it says all(*)
        3. Wait until it is done
    5. Log into backup router
        1. Look and ensure all services/rules/whatever have changed

Other Information

Do maintenance

One thing you can do with this setup is perform maintenance, with a fallback if something goes bump.

1. Update backup router
2. Open Primary Router
    1. Firewall | Virtual IPs | Status
        1. Click Enter Persistent CARP Maintenance Mode
        2. Your backup router is now master
3. Test everything on the new update. If it all works, update the master router, then turn off the CARP Maintenance Mode
4. **Note**: Persistent Mode survives a reboot. You must manually turn it off

Testing

Links

- https://docs.opnsense.org/manual/how-tos/carp.html