EN

High Availability with OPNsense and CARP

Active/Passive Pair with Zero Downtime

March 2026 | OPNsense Stack Series — Post 10

Table of Contents

1. What is CARP?

CARP (Common Address Redundancy Protocol) is a network protocol that allows multiple machines to share a virtual IP address (VIP). Originally developed for OpenBSD and integrated into OPNsense/pfSense, CARP ensures firewall high availability: if the master node fails, the standby node takes over within seconds, completely transparently to active connections.

In my BOTUM infrastructure, I use CARP for three critical scenarios:

- Zero-downtime OPNsense upgrades: fail over to backup, upgrade master, fail back
- Hardware or Proxmox VM failures: automatic failover in under 3 seconds
- Planned maintenance: clean master shutdown, backup takes over seamlessly

2. Prerequisites: 2 OPNsense VMs on Proxmox

- 2 identical OPNsense VMs on Proxmox (same version, same base configuration)
- 3 network interfaces per VM: WAN, LAN, and SYNC (pfsync)
- A dedicated switch or VLAN for the synchronization link
- SSH access to both nodes
- Identical OPNsense version on both nodes (mandatory)

Recommended Network Architecture

```
# OPNsense-1 (MASTER)
# - vtnet0 : WAN  -> IP: 203.0.113.2/28 (real)
# - vtnet1 : LAN  -> IP: 192.168.1.1/24 (real)
# - vtnet2 : SYNC -> IP: 192.168.254.1/30

# OPNsense-2 (BACKUP)
# - vtnet0 : WAN  -> IP: 203.0.113.3/28 (real)
# - vtnet1 : LAN  -> IP: 192.168.1.2/24 (real)
# - vtnet2 : SYNC -> IP: 192.168.254.2/30

# Shared CARP VIPs (clients use these IPs)
# - WAN VIP : 203.0.113.4/28  (VHID 1)
# - LAN VIP : 192.168.1.254/24 (VHID 2)
```

3. Configure CARP VIPs

Create WAN VIP on MASTER

In OPNsense MASTER: Interfaces > Virtual IPs > Add

```
# Interfaces > Virtual IPs > Settings > Add
Type         : CARP
Interface    : WAN
IP Address   : 203.0.113.4 / 28
Virtual VHID : 1
VHID Password: MyCarpPassword2026
Advertising frequency - Base: 1
Advertising frequency - Skew: 0   <- 0 = MASTER (high priority)
Description  : WAN-VIP-CARP
```

Create LAN VIP on MASTER

```
# Repeat for LAN interface
Type         : CARP
Interface    : LAN
IP Address   : 192.168.1.254 / 24
Virtual VHID : 2
VHID Password: MyCarpPassword2026
Advertising frequency - Base: 1
Advertising frequency - Skew: 0
Description  : LAN-VIP-CARP
```

Configure BACKUP (Skew 100)

```
# On OPNsense-2 (BACKUP) — same config, only skew changes:
# WAN VIP : VHID 1, Skew 100  <- 100 = BACKUP (low priority)
# LAN VIP : VHID 2, Skew 100

# CARP Priority Rules:
# - Skew 0   = high priority -> MASTER (active)
# - Skew 100 = low priority  -> BACKUP (standby)
# - Lower skew = higher priority
```

4. pfsync: Connection State Synchronization

pfsync synchronizes firewall state tables between both nodes in real time. During failover, active TCP connections (SSH, HTTPS, VPN) are not interrupted because the backup already knows all connection states.

Enable pfsync on MASTER

System > High Availability > Settings

```
# System > High Availability > Settings

[High Availability Sync]
  Synchronize States (pfsync)   : checked
  Synchronize Interface         : SYNC  (vtnet2)
  pfsync Synchronize Peer IP    : 192.168.254.2  <- BACKUP SYNC IP

[Firewall]
  Synchronize firewall rules    : checked
  Synchronize NAT               : checked
  Synchronize static routes     : checked
```

Enable pfsync on BACKUP

```
# System > High Availability > Settings (on BACKUP)

[High Availability Sync]
  Synchronize States (pfsync)   : checked
  Synchronize Interface         : SYNC  (vtnet2)
  pfsync Synchronize Peer IP    : 192.168.254.1  <- MASTER SYNC IP
```

i The SYNC link must be isolated on a dedicated VLAN or network. Never route user traffic through this interface.

5. XMLRPC Config Sync

XMLRPC Config Sync automatically propagates OPNsense configuration from MASTER to BACKUP. Every change on the MASTER (new firewall rule, NAT, alias) is synchronized without manual intervention.

Configure XMLRPC on MASTER

```
# System > High Availability > Settings

[Configuration Synchronization]
  Synchronize Config to IP    : 192.168.254.2  <- BACKUP SYNC IP
  Remote System Username      : root (or admin)
  Remote System Password      : BackupPassword2026

# Sections to synchronize (check all):
  Aliases        Certificates     DHCP Server
  DNS Resolver   Firewall Rules   Gateways
  Interfaces     NAT              OpenVPN / WireGuard
  Routes         Users and Groups
```

6. Testing Failover

Failover testing is MANDATORY before going to production.

Test 1: Graceful Failover

```
# System > High Availability > Status
# MASTER: CARP State = MASTER (VIPs active)
# BACKUP: CARP State = BACKUP (VIPs standby)

# Force MASTER to become BACKUP:
pfctl -d  # Temporarily disable firewall (forces failover)
# OR via interface:
# System > High Availability > Forcefully become BACKUP

# BACKUP promotes to MASTER in ~2-3 seconds
```

Test 2: Hard Failure Simulation

```
# In Proxmox, power off OPNsense-1 (MASTER) VM:
# qm stop 100  (or via Proxmox UI)

# On a network client, run continuous ping to VIP:
ping 203.0.113.4
# -> Expect 1-2 packet losses maximum during failover
# -> Backup takes over in 1-3 seconds

# Verify on BACKUP:
# VIP WAN: MASTER | VIP LAN: MASTER  OK
```

Test 3: Active Connections Survive Failover

```
# On a client, open SSH session via LAN VIP:
ssh admin@192.168.1.254

# While SSH session is open, force failover
# SSH session MUST SURVIVE thanks to pfsync
# (TCP states are synchronized in real time)

# If SSH survives -> pfsync works correctly
# If SSH drops    -> check pfsync configuration
```

7. Production Use Cases

Zero-Downtime OPNsense Upgrade Procedure

```
# Step 1: Verify backup is healthy
#    System > High Availability > Status
#    BACKUP: CARP BACKUP, pfsync OK, config synced

# Step 2: Fail over traffic to BACKUP
#    MASTER: System > HA > Forcefully become BACKUP
#    -> BACKUP becomes MASTER, takes all VIPs

# Step 3: Upgrade former MASTER (now BACKUP)
#    System > Firmware > Updates > Upgrade
#    -> Normal reboot, no traffic impact

# Step 4: Verify MASTER return
#    -> Returns to BACKUP mode automatically
#    -> Verify state sync + config sync OK

# Step 5: Repeat for second node
#    Result: Both nodes upgraded, 0 seconds downtime
```

8. CARP Monitoring with Grafana

Integration with the Grafana + InfluxDB stack from Post 9 to monitor CARP state in real time.

Collect CARP Metrics via Telegraf

```
# In telegraf.conf (on monitoring server):
[[inputs.http]]
  urls = ["http://OPNSENSE-VIP/api/diagnostics/interface/getVipStatus"]
  method = "GET"
  username = "telegraf_user"
  password = "YOUR-API-TOKEN"
  data_format = "json"
  name_suffix = "_carp"

# Grafana Flux query - CARP state:
from(bucket: "opnsense")
  |> range(start: -1h)
  |> filter(fn: (r) => r._measurement == "http_carp")
  |> filter(fn: (r) => r._field == "status")
```

Recommended Dashboard Panels

- Current CARP state (MASTER/BACKUP) per VIP — Gauge
- Failover history — Timeline/Log panel
- pfsync counter: states synced/second — Time series
- SYNC link latency — Gauge (alert if > 10ms)
- Number of synchronized firewall states — Stat panel

9. Next Steps — SIEM Wazuh

You now have a high-availability OPNsense infrastructure, resilient to failures and maintenance. The next step in the series is Post 11: SIEM integration with Wazuh to centralize security logs and detect intrusions.

Full article: blog.botum.ca/opnsense-carp-high-availability-guide

Website: www.botum.ca |

— Canada