Step by step Guide

Configuration Steps

1. **Disable Outbound NAT Rule Generation**
   Navigate to **Firewall > NAT > Outbound** and select **Disable Outbound NAT rule generation**. This ensures that the firewall doesn't alter the source IP addresses of packets passing through the bridge.
2. **Adjust System Tunables**
   Go to **System > Settings > Tunables** and modify the following parameters:
   - Set `net.link.bridge.pfil_bridge` to `1` to enable filtering on the bridge.
   - Set `net.link.bridge.pfil_member` to `0` to disable filtering on the individual interfaces.
3. **Create the Bridge Interface**
   Navigate to **Interfaces > Other Types > Bridge** and add a new bridge. Select the interfaces you wish to include in the bridge (e.g., LAN and WAN).
4. **Assign a Management IP**
   Go to **Interfaces > Assignments**, select the newly created bridge interface, and assign it an IP address for management purposes.
5. **Disable Block Private Networks & Bogons**
   In **Interfaces > [Bridge]**, uncheck the options for **Block private networks** and **Block bogon networks** to allow all IP addresses to pass through the bridge.
6. **Disable DHCP Server on LAN**
   Ensure that the DHCP server is disabled on the LAN interface to prevent it from assigning IP addresses to devices connected to the bridge.
7. **Add Allow Rules**
   Navigate to **Firewall > Rules > [Bridge]** and add rules to allow traffic as needed. For a basic setup, you can allow all traffic to pass through.
8. **Disable Default Anti-Lockout Rule**
   In **Firewall > Rules > [Bridge]**, disable the default anti-lockout rule to prevent being locked out of the management interface.
9. **Set Interface Types to 'None'**
   Go to **Interfaces > [LAN]** and **Interfaces > [WAN]**, and set the interface types to **None**. This ensures that these interfaces are part of the bridge and not assigned IP addresses.
10. **Apply Changes**
    After completing the above steps, apply the changes to activate the transparent filtering bridge.

?? Important Notes

- During the configuration process, you will be prompted to apply changes multiple times. It's crucial to save all changes before applying them to avoid losing access to the management interface.
- Ensure that the firewall rules are correctly configured to allow necessary traffic; otherwise, you may inadvertently block legitimate connections.

You can also find Opnsense documentation Here

Revision #1
Created 2025-10-13 01:23:26 UTC by Dale
Updated 2025-10-13 01:26:20 UTC by Dale