Transparent Firewall/Filtering Bridge - pfSense 2.0.1

By William Tarrh

Version 1 – November 28, 2012

Transparent Firewall/Filtering Bridge - pfSense 2.0.1

This "how to" is an updated version of Trendchiller's 2007 *How to Setup a transparent firewall /filtering bridge with pfSense* based on **pfSense 1.0-PREBETA2-BUG-VALIDATION-EDITION**.

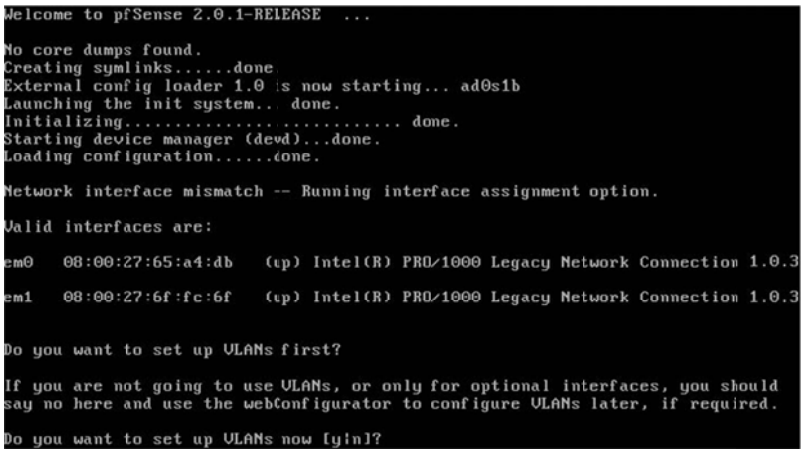
My contribution to this project is documenting what has been noted by others on the pfSense forum, walking in Trendchiller's footsteps and the submission of the document itself.

Special thanks to Chris Buechler, Scott Ullrich and all of those who contribute to the pfSense Forum. I would also like to thank Dr. Jeff Rattray who helped me work through some of the kinks in this project.

Contents

1. **Hardware Requirements and Setup**
   a. Two compatible NIC's for the LAN and WAN interfaces.
      pfSense Hardware Compatibility

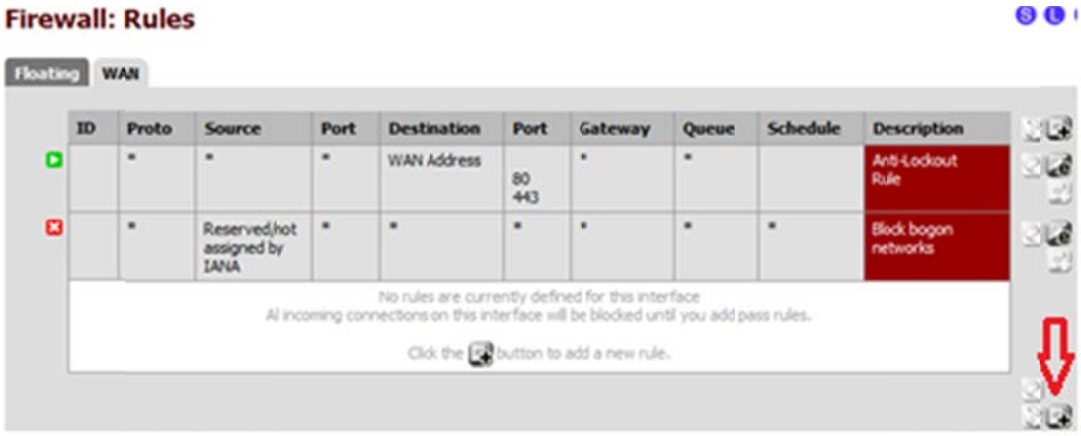
2. **Initial Setup**
   a. Upon completing a fresh installation of pfSense a restart will be required. After the first reboot you will be greeted with **"Do you want to set up VLANs now [y|n]?"** Select **"No"**.



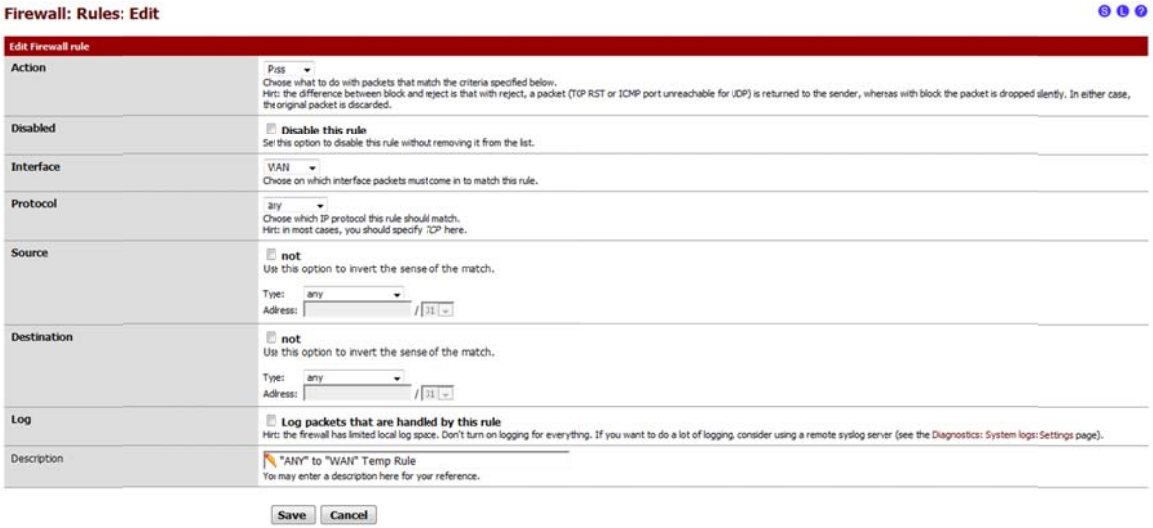
   b. Next you will be requested to select your **WAN** interface or select **'a'** for auto detection. Select your desired **WAN** interface card from the list. Next you will be asked to select your **LAN** interface card. Press **"Enter"**, we will configure this interface later.
   c. At the welcome screen only setup the **WAN** interface. Assign this adapter a static address or use the assigned DHCP address; we will use this address to configure the firewall from this point on.

3. **pfSense GUI Login**
   a. Open a browser window and enter the IP address assigned to the pfSense **WAN** interface. The default username and password are **admin** and **pfsense**.

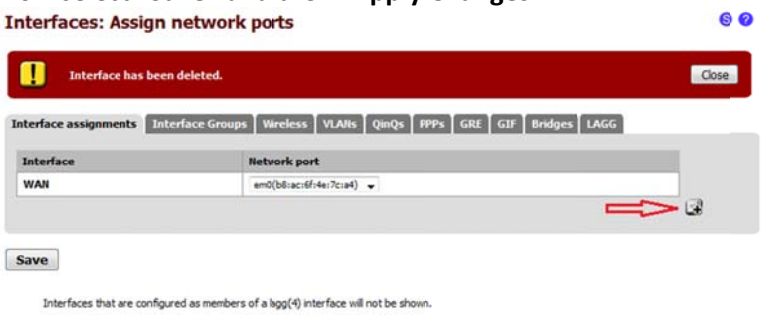
4. **Firewall – WAN - Anti-Lockout Rule**
   a. First, let's be sure not to get locked out of the **WAN** interface by setting up our own temporary "**anti-lockout**" rule. Navigate to **"Firewall" -> "Rules"**. By default the **"Anti-Lockout"** rule is applied to the **WAN** interface as seen below. As soon as the **LAN** interface is enabled this **"Anti-Lockout"** rule will be migrated automatically to the **LAN** interface.
   b. To create a new rule, select the **'+'** on the bottom right-hand corner. This will take you to the **Rules: Edit** page**.**



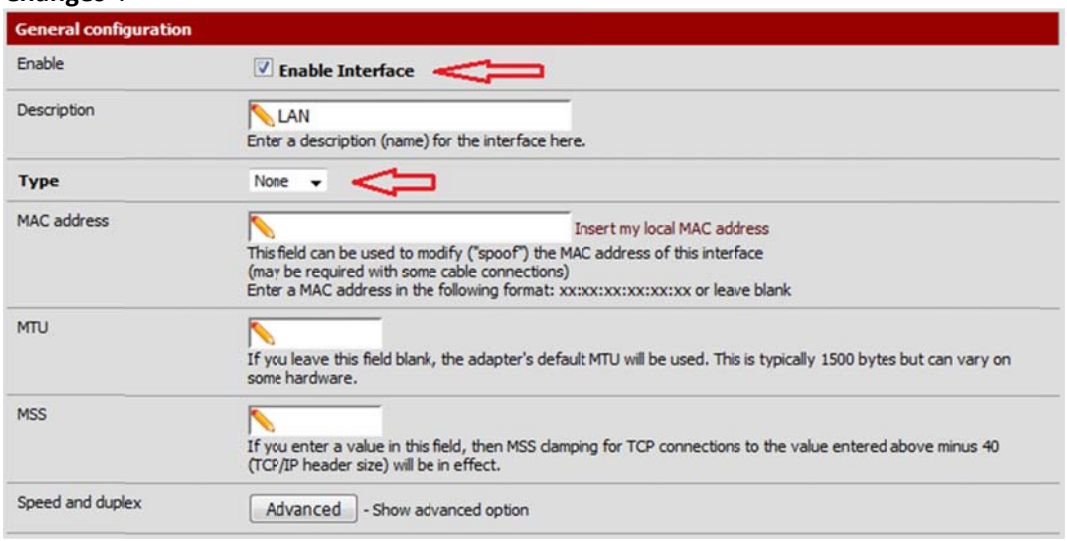
In the **"Rules: Edit"** create a rule that resembles the screen shot below. The rule below will allow all traffic to access the **WAN** interface. Keep in mind this is a temporary rule. Select **"Save"** and then **"Apply Changes"**.



5. **Enable and Configure LAN Interface**
   a. Navigate to **"Interfaces" -> "(assign)"**. Select the **'+'** and then select your **"LAN"** interface. Now select **"Save"** and then **"Apply Changes"**.

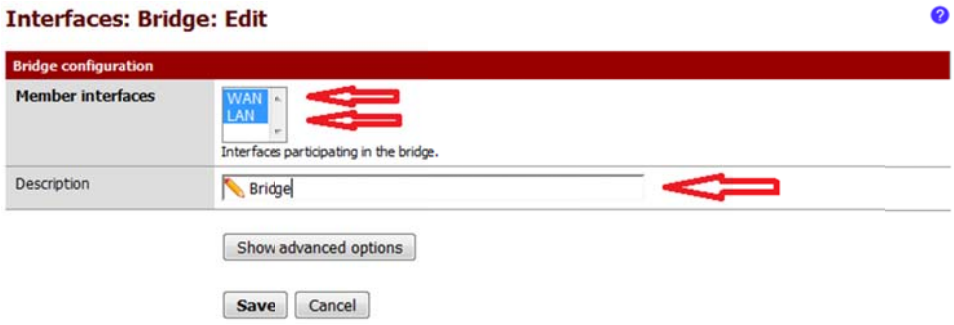


Navigate to **“Interfaces” -> “LAN”**. In **General configuration** check the **“Enable Interface”** box. The screen will auto populate. Be sure that **Type** is set to **“None”**. **“Save”** and **“Apply Changes”**.

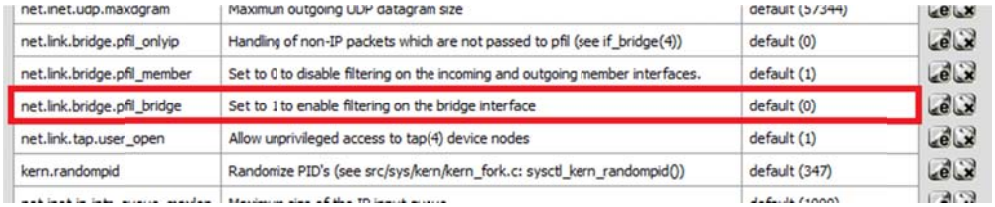


6. **Enable and Configure the Bridge**
   a. Now that our **LAN** and **WAN** interfaces are enabled and configured we can create the Bridge. Navigate to **“Interfaces -> (assign)”** from the menu and then select the **“Bridges”** tab to the far right. Select the **‘+’** to navigate to **“Bridge:Edit”**.

In **“Bridge: Edit”** hold the **“Ctrl”** key on your keyboard and select the **“WAN”** and **“LAN”** so they are both highlighted. Assign your Bridge a name in the **“Description”** field. Select **“Save”** and then **“Apply Changes”**.

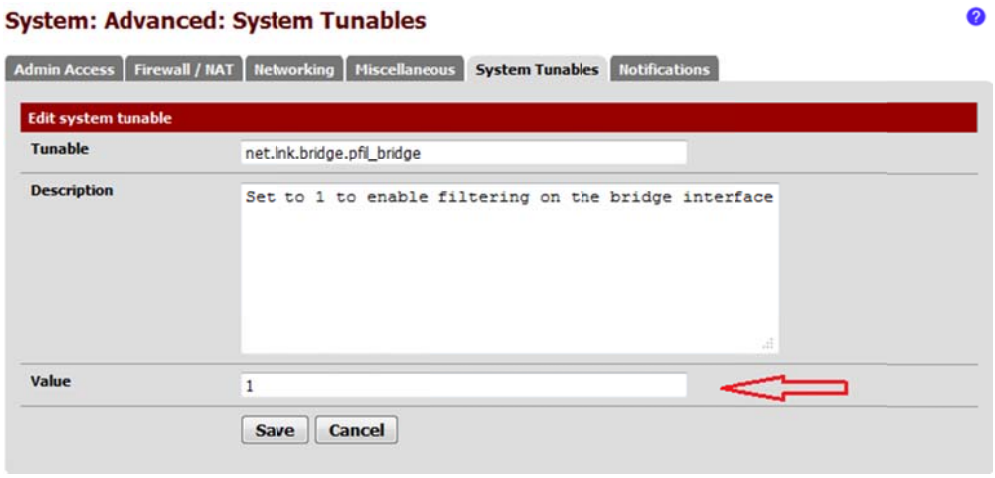


7. **Enable the Filtering Bridge**
   a. In the menu navigate to **"System -> Advanced"** and select the **"System Tunables"** tab.
   b. Locate the **"net.link.bridge.pfil_bridge"** in the **"Tunable Name"** column and double-click it.

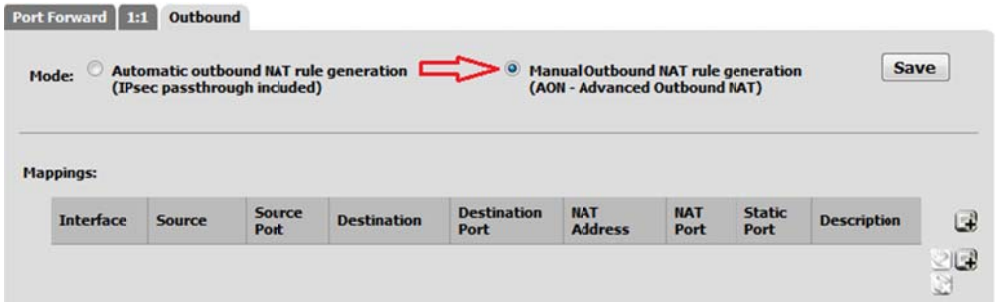


net.inet.udp.maxdgram	Maximum outgoing UDP datagram size	default (57344)
net.link.bridge.pfil_onlyip	Handling of non-IP packets which are not passed to pfil (see if_bridge(4))	default (0)
net.link.bridge.pfil_member	Set to 0 to disable filtering on the incoming and outgoing member interfaces.	default (1)
net.link.bridge.pfil_bridge	Set to 1 to enable filtering on the bridge interface	default (0)
net.link.tap.user_open	Allow unprivileged access to tap(4) device nodes	default (1)
kern.randompid	Randomize PID's (see src/sys/kern/kern_fork.c: sysctl_kern_randompid())	default (347)

   c. In the **"Value"** field change this from **"Default"** to **"1"**. Select **"Save"** and **"Apply Changes"**.

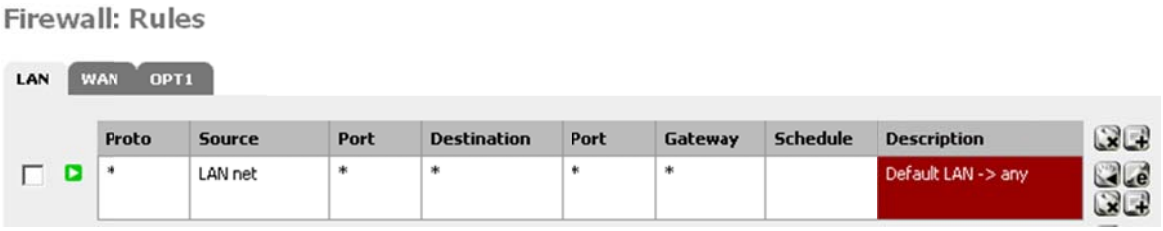


8. **Enable Manual outbound NAT rule generation (AON – Advanced Outbound NAT)**
   a. From the menu select **"Firewall -> NAT"** and the **"Outbound"** tab.
   b. Click **"Manual outbound NAT rule generation (AON – Advanced Outbound NAT)"** and select **"Save"**. Delete any rules that auto-populate in the mappings area.



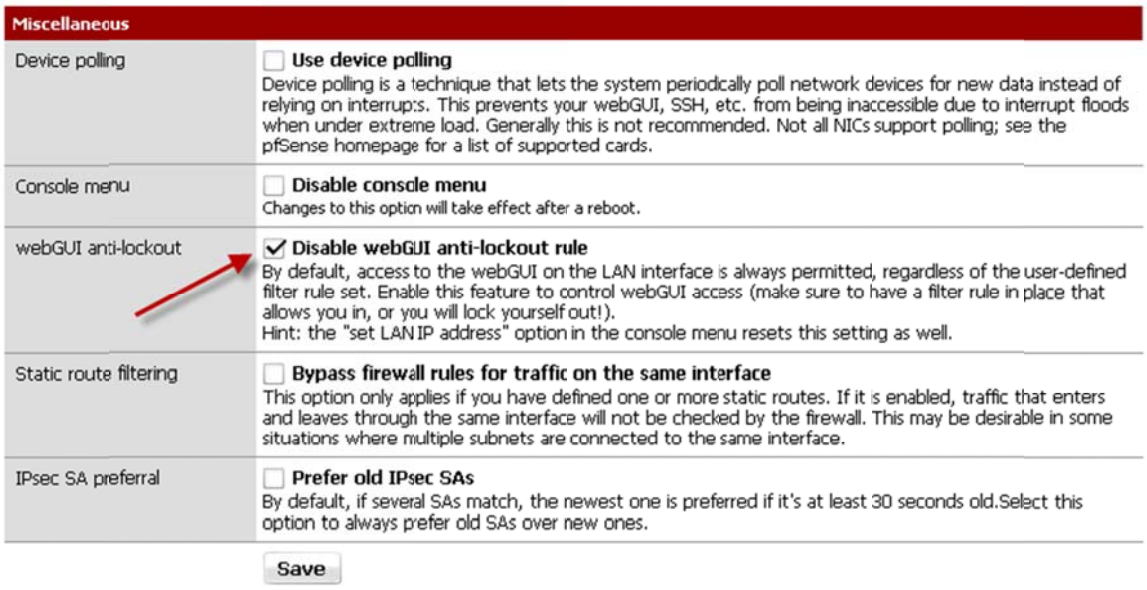
9. **Reboot pfSense Firewall**
    a. In order to fully apply all changes reboot your pfSense firewall by going to **“Diagnostics -> Reboot”**. In this menu select **“Yes”**.

10. **Restrict Access to the Management Interface**
    a. This documentation was taken from doc.pfsens.org, I found it to be very helpful. http://doc.pfsense.org/index.php/Restrict_access_to_management_interface

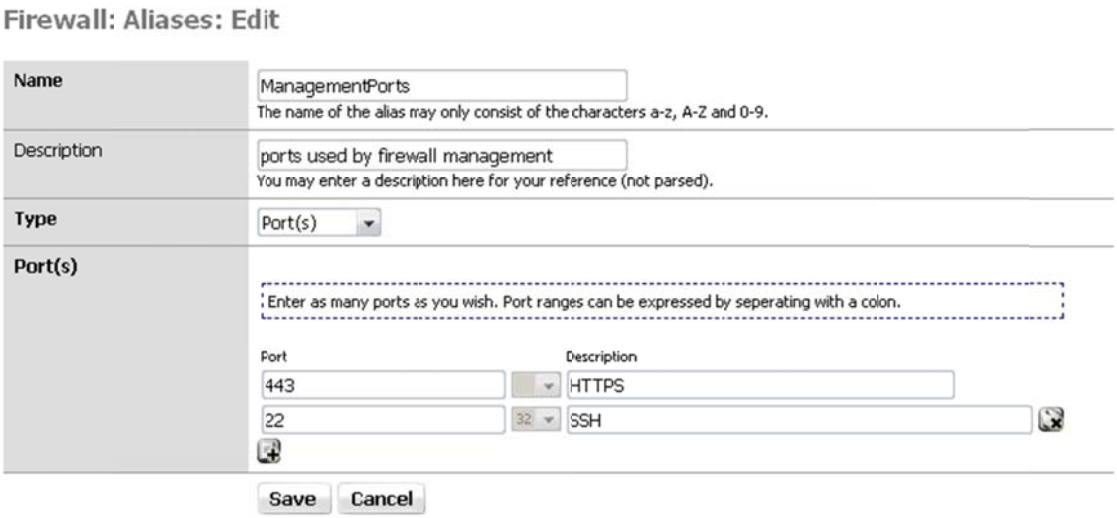


If you use a restrictive ruleset on your LAN, make sure it permits access to the web interface before continuing.

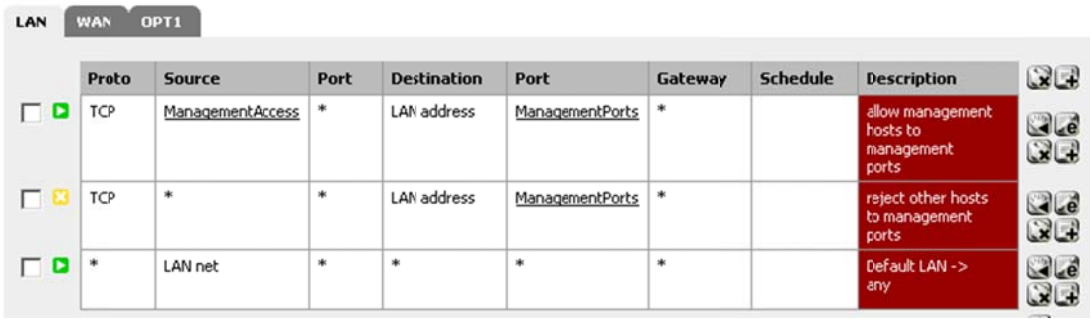
Now disable the anti-lockout rule by going to the System -> Advanced page and checking the "Disable webGUI anti-lockout rule" box. Click Save and the rule will be removed.



Now I suggest adding a network alias for management access, and if you use both web and SSH administration, add an alias for those ports.



Now add a firewall rule allowing the sources defined in your management alias to the destination LAN address, with the port used or alias created for those using multiple ports. Make sure this rule comes first in the list. Then add a rule based on that rule (the + next to the rule), changing action to block or reject (I prefer reject on internal networks), source to any, and destination the same. When finished your ruleset should look like the following.



Apply your changes and your management interface is now restricted to only the defined hosts.

11. Overview and Understanding of the Transparent Bridge

I use the **WAN** as the management interface because I was unable to reach anything external, obtain updates or browse packages when the **LAN** or **Bridge** was configured as the management interface.

Treat the **LAN** and **WAN** interfaces as you would a standard firewall, keep in mind that the default action in the transparent bridge is to **block** all traffic unless explicitly allowed in the firewall. You will only need to setup rules on the **LAN** and **WAN**, I have yet to touch the **Bridge**.

Generally a standard firewall will allow the **LAN** to **ANY** by default; this will allow anything on the LAN outbound. In this transparent bridge scenario you **MUST** create a rule to allow your **LAN** outbound. As stated above the default behavior of the transparent bridge is to block unless explicitly allowed.