# pfSense - Bug #2367

## display negate rules in firewall_rules.php and evaluate when added

04/11/2012 12:02 AM - Chris Buechler

| | | | |
|---|---|---|---|
| **Status:** | New | **Start date:** | 04/10/2012 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | Rules / NAT | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **Affected Version:** | All | **Affected Architecture:** | |

**Description**

the fact the negate policy routing rule isn't shown is bad as it has lead to unintended consequences (ends up passing traffic people don't realize is passed because it's hidden). They should be shown as a grayed out auto-added rule, similar to block private/bogon.

Also need to look at when and how that rule is automatically added. In some circumstances it can allow more traffic than the user intends, such as:
http://forum.pfsense.org/index.php/topic,48143.0/topicseen.html

### History

#### #1 - 04/11/2012 07:33 AM - Jim Pingle

*- Subject changed from display netgate rules in firewall_rules.php and evaluate when added to display negate rules in firewall_rules.php and evaluate when added*

#### #2 - 04/12/2012 05:45 AM - Seth Mos

Normally the NEGATE rules will only trigger when the destination is set to "any".

If we change the foreach($config['rules'] as $rule) to a function that returns the firewall rules it should be easier to tack on NEGATE rules, add other rules, all in a fashion that they will also show in the UI.

e.g.

```
return_firewall_rules() {
 $rules = array();
 $rules = $rules + add_bogon_rules();
 foreach($config['rules'] as $rule) {
  if($negate)
   $rules[] = $negate_rule;
  $rules[] = $rule;
 }
 $rules = $rules + add_v6_delegation_rules();
}
```

For example. The automatic rules I added for dynamic IPv6 connections need to shown as well. It's less then optimal.

**#3 - 05/07/2012 06:11 PM - Chris Buechler**

*- Target version deleted (2.1)*