PFSense Checklist

Here are handy links

[Securing the system](#_gjdgxs)

[Change admin password](#_30j0zll)

[Set up the firewall](#_1fob9te)

[Web Gui Method](#_26in1rg)

[Inbound Rules](#_3znysh7)

[Outbound Rules](#_2et92p0)

[Other things to check](#_tyjcwt)

[Troubleshooting](#_3dy6vkm)

[EXAMPLE: SSH Firewall Inbound Rule](#_1t3h5sf)

[Port/Protocol Table](#_3rdcrjn)

### Securing the system

#### Change admin password

* 1. In a browser on a machine with a GUI, navigate to the pFSense machine’s IP address. Ignore the unsafe connection notification.
  2. **Note:** There may be a prompt. In that case, ignore the rest of these steps and just click the prompt.
  3. Log in with default credentials
     1. Username: “admin”
     2. Password: “pfsense”
  4. On the top bar, click over “System” and select “User Manager”
  5. Click the edit button
     1. Looks like this  in old pfsense and this  in newer versions.
  6. Change the password
     1. Log out and back in to confirm

#### Set up the firewall

[*There’s an example at the bottom of this document*](#_1t3h5sf)

* 1. Log in to the web gui
  2. On the top bar or hamburger menu, click “Firewall” and select “Rules”

###### Inbound Rules

* + 1. Click “Add.” This one will allow the scored services through
       1. For Action, select “Pass”
       2. For interface, select the previously selected one
       3. For protocol, select the applicable service. It can be found in the table below
       4. For Source, select “Any”
       5. For Source Port, select “Any”
       6. For Destination, select “Single host or alias”, and fill in the IP address of the box that the service you’re configuring the rule for applies to. If using NAT, be sure to use the internal address of the system.
       7. For each of the services [in the table below](#_2s8eyo1) that are applicable to your competition, select the port(s) and description necessary for your service. (Note: You can click the icon to create a new rule based on an old rule. This way, you just have to change the ports and/or protocol)

###### Outbound Rules

**Note:** The only things you really need for outbound rules are DNS, HTTP, HTTPS, and FTP. These are created exactly the same as inbound rules **except** the interface **isn’t** the one facing red ream and the scoreboard. It’s the one facing your vApp’s machines. It will likely be “LAN”

* + 1. Click “Add.” This one will allow the interwebs and FTP out
       1. For Action, select “Pass”
       2. For interface, select the internal one (Probably “LAN”)
       3. For protocol, select the applicable service. It can be found in the table below
       4. For Source, select “Any”
       5. For Source Port, select “Any”
       6. For Destination, select “Single host or alias”, and fill in the IP address of the box that the service you’re configuring the rule for applies to.
       7. For each of the services [in the table below](#_2s8eyo1) that are applicable to your competition, select the port(s) and description necessary for your service. (Note: You can click the icon to create a new rule based on an old rule. This way, you just have to change the ports and/or protocol)
    2. **IMPORTANT THING TO NOTE**
       1. **Hit “Apply Changes”**

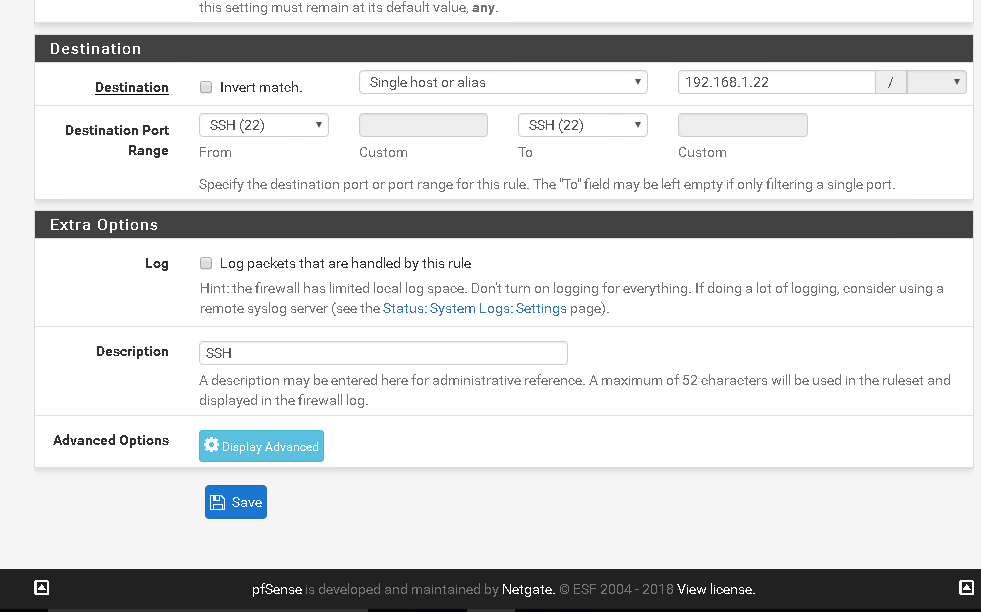
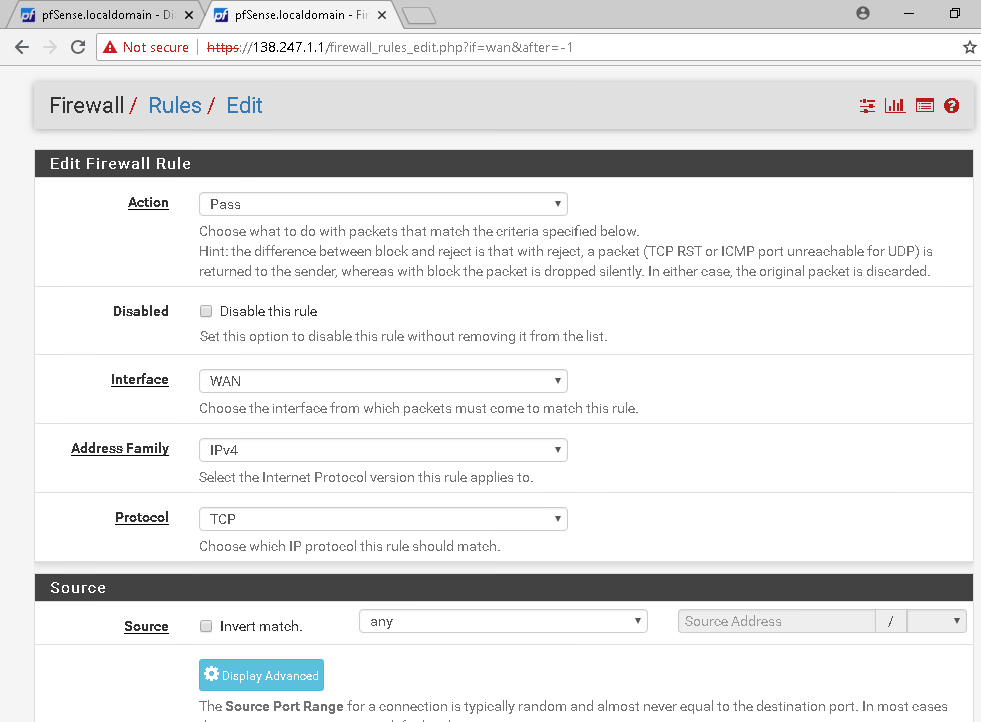
#### Other things to check

* 1. If there’s an “Allow All” rule there when the box is booted up, disable it.
  2. Get rid of extra users
     1. On the top bar, click over “System” and select “User Manager”
     2. Click the  icon next to the unwanted user
     3. Check the “Disabled” box at the top of the screen
     4. Click “Save” at the bottom of the page
     5. If prompted, click “Apply Changes”

#### Troubleshooting

* 1. On the top bar, click over “Diagnostics” and select “Packet Capture”
     1. brother

### EXAMPLE: SSH Firewall Inbound Rule

SSH Server’s IP is 192.168.1.22

### 

### 

### 

### Port/Protocol Table

[Here’s a link back to firewall rules if you’re switching back and forth](#_1fob9te)

| Description | Protocol | Inbound Ports | Outbound Ports |
| --- | --- | --- | --- |
| Web\_Ports | TCP | 80, 443, 8080 | 80, 443, 8080 |
| SSH\_Port | TCP | 22 |  |
| Email\_Ports | TCP | 143, 25 |  |
| FTP\_Ports | TCP | 21,65500:65502 | (unnecessary for most mocks) 20 |
| LDAP\_Port | TCP/UDP | 389 |  |
| DNS\_Port | TCP/UDP | 53 | 53 |
| MySQL\_Port | TCP | 3306 |  |
| MSSQL\_Port | TCP/UDP | 1433 |  |
| SMB\_Port | TCP | 445 |  |
| RDP\_Port | TCP/UDP | 3389 |  |