PRINT QUESTION

This article is also available for viewing online at http://kb.mosaicdataservices.com/questions/149/

Managing the APF Firewall on Shared Linux Servers

Advanced Policy Firewall, or **APF**, is a firewall sometimes seen on Mosaic's Linux VPS and Dedicated servers. It is basically an interface to iptables, which is the standard interface to managing network ports on Linux machines. Interacting with iptables can be complex and error-prone, and **APF** greatly simplifies working with it. However, **APF** is still only accessible by ssh. There is no way to make changes in **APF** through WHM or cPanel.

All of the **APF** configuration files are located in the **/etc/apf** folder on the shared server. Within this folder the **allow_hosts.rules** file contains all of the IP addresses that are whitelisted for the server and the **deny_hosts.rules** file contains all of the IPs that are being blocked by the firewall. Within the **deny_hosts.rules** file each IP that is being blocked should also include a reason behind the block(most of them will be blocked by bfd, which blocks IPs attempting to brute force the server).

GLOBAL DENY / ALLOW LISTS

We are are now managing our own GLOBAL ACCESS AND DENY rules so it is important that you check both places when attempting to remove an IP address from a server or whitelisting an IP address.

I have set up a repository for Global Deny rules that will be integrated into the APF Firewall on all linux shared hosting servers.

The global_deny.rules for Mosaic Data is located on Linux 4 at:
http://www.mosaicdataservices.com/download/apfbfd/glob_deny.rules

The global_allow.rules for Mosaic Data is located on Linux 4 at:
http://www.mosaicdataservices.com/download/apfbfd/glob_allow.rules

The block lists we use is taken from Wizcraft:
http://www.wizcrafts.net/iptables-blocklists.html

If you ever have to edit the global_deny.rules for any reason, you have to edit the file on the MDS website (above) and then restart APF on the server for it to take affect.

If you make a change to the GLOBAL ALLOW OR DENY LISTS you must restart APF on specific servers in order to have it take affect using:
#apf -r

MANAGING APF FIREWALL

Starting, stopping, and restarting apf can be easily done via the command line:

apf -s This will start apf if it is not running.

apf -r This will restart apf.

apf -f This will stop apf and flush all rules from the firewall.

Black-listing an IP

To block an IP in the firewall on a specific server, simply ssh in as root and run the following command:

```
apf -d 127.0.0.1
```

If the IP has previously been whitelisted, that command will give you this error:

```
127.0.0.1 already exists in /etc/apf/allow_hosts.rules
```

You'll need to open /etc/apf/allow_hosts.rules in your preferred text editor and remove the IP before you can block it in the firewall. If your setup is more recent, this command may work to get the IP out of allow_hosts.rules:

```
apf -u 127.0.0.1
```

To blacklist an IP address globally, you will need to add it to the global_deny.rules list on Linux 4 (see above) and restart APF on the specific server for it to take affect. This will block the IP / Subnet on ALL servers that use the global_deny.rules ruleset.

White-listing an IP

If you have an IP address that you would like never to be added to the firewall (also known as whitelisting), simply run this command as root:

```
apf -a 127.0.0.1
```

(be sure to replace 127.0.0.1 with the IP address in question)
If the IP address is currently being blocked by the firewall, you will get an error:

```
127.0.0.1 already exists in /etc/apf/deny_hosts.rules
```

If that happens, you will need to open /etc/apf/deny_hosts.rules in your favorite text editor and remove the IP address before it can be added to the whitelist. If your setup is more recent, you may be able to run the following to remove the IP address from deny_hosts.rules:

```
apf -u 127.0.0.1
```

To whitelist an IP address globally, you will need to add it to the global_allow.rules list on Linux 4 (see above) and restart APF on the specific server for it to take affect. This will allow the IP / Subnet on ALL servers that use the global_allow.rules ruleset.

Opening a port in the apf firewall

By default apf is configured in such a way that all ports are blocked besides the ones specifically allowed to be open to the world. To allow access to additional ports, the main apf configuration file needs to be edited.

Please be advised that making a change to the apf configuration file has to be done via hand at the command line. If you do not feel comfortable making these changes feel free to contact a systems administrator at Liquid Web to assist with any configuration changes that need to occur.

First open the apf.conf file
`vim /etc/apf/conf.apf`
Within this file the file that needs to be changed starts with IG_TCP_CPORTS= and looks like this:

```
IG_TCP_CPORTS="20,21,22,25,53,80,110,143,443,465,993,995,2082,
2083,2084,2086,2087,2095,2096,3306,3784,7786,30052"
```

Now this line needs to be edited to include the additional port.

- Within vim hit **a** to enter insert mode.
- Within insert mode add the additional port to the current list followed by a comma.
- Now hit escape(**esc**) to exit insert mode.
- To write and save the changes type **:wq** and hit enter.
- After these changes have been done restart apf with this command: **apf -r**

These instructions are for opening a TCP port. If a UDP port also needs to be opened up the instructions are the same except the line that needs be edited is the **IG_UDP_CPORTS** line.