Firewall: IPFWADM mini-howto

IPFWADM Mini-howtoIntroduction
FREESCO uses the IPFWADM firewall, which has a lot of options and could be tricky to configure.
Here is a list of all commands:

```
ipfwadm 2.3.0, 1996/07/30    Usage: ipfwadm -A [direction] comm
```

If you want to view these commands on your freesco, just type:

```
ipfwadm -h | more
```

This will display the general IPFWADM help (devided in 2 "pages")
Where to configure?
If you want to configure a firewall yourself, you should know what you are doing, otherwise you could end up with a router that is no longer reachable or worse one that is wide open to the internet!.

The best way to configure your firewall rules is to put them in the **/rc/rc_user** file in order for the changes to survive a reboot.

By adding your rules in the rc_user file, your rules will be loaded BEFORE the standard freesco rules are loaded.

Firewall rules will be "read" from the TOP of the list to the BOTTOM of the list. If the firewall encounters a rule that matches specific traffic, it will apply that rule and look no further.

Therefore it is nececarry to put "allow" rules BEFORE "deny" or "reject" rules!
example

```
ipfwadm -I -a reject -P all -S 0/0 -D 192.168.0.0/24

ipfwadm -I -a accept -P tcp -S 0/0 -D 192.168.0.1/32 25
```

In the first rule you block all traffic from anywhere to the 192.168.0.x range (192.168.0.0 to 192.168.0.255)

therefore the accept rule for tcp port 25 traffic to the 192.168.0.1 system WILL NOT WORK !

After you edited your rules, type:

rc_masq restart

to reload the firewall rules.

The basics
The next firewall rule will be described here in detail:

```
ipfwadm -I -a reject -P tcp -W $INET -D 0.0.0.0/0 22 -y -o
```

Of course we start with the general command

IPFWADM

The "traffic" direction this rule is for (-I)

-I Inbound traffic (traffic TO your router)
-O Outbound traffic (traffic FROM your router)

The way this rule should be applied into the firewall rule set (-a)
-a The rule will be appended (added) in the list or current rules.
-I The rule will be inserted into the current rules list

I don't know what the difference is here, but Since I created my own special rule-set... I use the -a option.

The policy regarding the traffic (reject)

accept The rule will allow this specific traffic
reject The rule will reject this specific traffic, but will send a response to the other side saying this port is "closed"
deny The rule will deny this specific traffic, and will not send any response (stealth)

The Protocol identifier (-P)
-P The actual protocol used in the rule (if any)

The Protocol (tcp)

tcp The rule is used for TCP protocol
udp The rule is used for UDP protocol
icmp The rule is used for ICMP protocol
all The rule is used for ALL protocols

The source of the traffic (-W $INET)

-W $INET This stands for your INTERNET interface, and can be used if you want to block something from the INTERNET.
-S 0.0.0.0/0.0.0.0 This should be the Source IP the traffic is generated from, WITH subnet mask
-S 0.0.0.0/0 This should be the Source IP the traffic is generated from, WITH prefix

The destination of the traffic

-D 0.0.0.0/0.0.0.0 This should be the Destination IP the traffic is going to, WITH subnet mask
-D 0.0.0.0/0 This should be the Destination IP the traffic is going to, WITH prefix

The port (range)

22 The port you want the rule to apply to
22:25 The port range you want the rule to apply to

Filtering and logging
-y This will filter the packets which apply to this rule
-o This will log the rule into your log file if the rule is applied to traffic.

Example

reject incoming tcp connections to port 22 from the internet and log

should be:

ipfwadm -I -a reject -P tcp -W $INET -D 0.0.0.0/0 22 -y -o

As you can see...

ipfwadm is the basic command

-I is used because the rule must apply to INBOUND traffic (going TO the router)
-a is used to APPEND (add) this rule to your firewall rule-set (loaded on bootup)
reject is used because you want to BLOCK the inbound traffic. This still makes the router send a “port is in use, but closed” signal to the requesting ip.
-P tcp is used because you want to block a specific port on the TCP protocol

NOTE!
You CAN NOT specify a port WITHOUT specifying a protocol!

-W $INET is used because you want to block the traffic coming FROM the internet TO you internet interface

You could also use -W eth0 if your internet interface is eht0.

Or you could specify your public ip -S 198.133.219.25/255.255.255.255 or -S 198.133.219.25/32

198.133.219.25 should be replaced with your public ip address and 255.255.255.255 subnet mask is the same as /32 prefix, which means you specify just this 1 (one) ip address.

(search google for "tcp/ip subnetting" if you want to know more about that)

-D 0.0.0.0/0 is used to specify the destination ip address. In this case we block ALL ip ranges.

Instead of using 0.0.0.0/0 you could use 0/0, or 0.0.0.0/0.0.0.0 it's all the same.
If you would like to block the traffic to a specific range, you just specify the range:

-D 192.168.0.0/255.255.255.0 (with subnet mask) or the same range 192.168.0.0/24 (with prefix)

22 is used to specify the port.

If you want to block a range of ports, say 22 to 25 you should use the following:

22:25

NOTE! In order to specify a port (range), YOU NEED TO SPECIFY A PROTOCOL !

-y is used to specify that the packets should be filtered. This is not necessary and could cause problems! So I suggest you don't use it.

-o is used to put an entry in your freesco log file, each time the rule is applied.

NOTE!
If you put this in a rule for a port which is used very often (like a port used for gaming), your log files will flood and fill up with entries of this rule being applied!
(in other words... DON'T use this rule for multiplaying online or such things)

Unique solution ID: #1062
Author: Thasaidon
Last update: 2009-08-18 11:27