

**Block internet access for an IP** 28 posts [1](#) [2](#) [>](#)

**Post Reply**  Search this topic...

**Block internet access for an IP**  
 by **bloater99** » October 17th, 2014, 3:59 pm

I'm having trouble setting up a firewall rule to block internet access for a single machine with a fixed IP. Here is what I've done:

1. Create a firewall rule
2. Source is the IP address of the machine I want to only have LAN access.
3. Destination is Firewall (RED)
4. Protocol=ALL and DROP
5. Additional Setting: set rule position to 1 and Activate Rule.
6. Click Update

I then RDP to the machine in question and test ping to the internet and it still pings google.com

If it matters, I do not have NAT checked in the rule.

What am I doing wrong?

Thanks.

**bloater99**  
 Posts: 482  
 Joined: October 13th, 2014, 3:47 pm



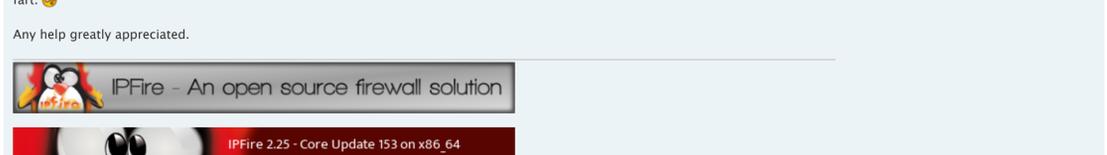
**Re: Block internet access for an IP**  
 by **bloater99** » October 17th, 2014, 6:16 pm

I've also tried with the source as the RED interface and destination the machine. I am attaching a screenshot. In each case, after I update the firewall rule and hit "apply" that machine still has internet access.

On a side note, I don't understand the significance of the "Policy: Blocked" and "Policy: Allowed" in my screenshot. Since both are set to Drop I would expect them both to say "Policy: Blocked". Can someone explain what this really means? I must be having a serious brain fart. 😊

Any help greatly appreciated.

**bloater99**  
 Posts: 482  
 Joined: October 13th, 2014, 3:47 pm



**Re: Block internet access for an IP**  
 by **trymes** » October 17th, 2014, 7:19 pm

By selecting "Firewall: RED" as the destination, you have told the firewall to block all requests from that computer to services hosted directly on your firewall's RED interface (like the WUI). In other words, if you try to reach your own external IP from that computer, you will not be able to.

To block outbound access, you should choose "Standard Networks: RED" instead.

When configuring firewall rules, don't forget that the order is important. Whichever rule matches first will be the one that is used.

Tom.

**trymes**  
 Posts: 664  
 Joined: February 9th, 2011, 4:10 pm  
 Location: New England, USA

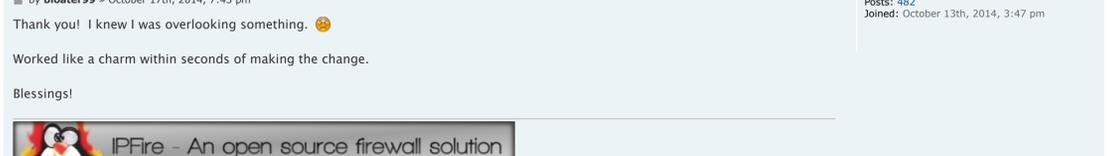
**Re: Block internet access for an IP**  
 by **bloater99** » October 17th, 2014, 7:43 pm

Thank you! I knew I was overlooking something. 😊

Worked like a charm within seconds of making the change.

Blessings!

**bloater99**  
 Posts: 482  
 Joined: October 13th, 2014, 3:47 pm



**Re: Block internet access for an IP**  
 by **trymes** » October 17th, 2014, 8:07 pm

Hey! Every once in a while I get one right. Good luck!

**trymes**  
 Posts: 664  
 Joined: February 9th, 2011, 4:10 pm  
 Location: New England, USA

**Re: Block internet access for an IP**  
 by **catbit** » October 17th, 2014, 8:17 pm

I tested something like bloater99, but in my case it doesn't work.

source: local ip  
 destination: standard networks RED  
 protocol: all and DROP

click on Update and then Apply but the notebook on that local ip still have internet access.

What I'm doing wrong?

**catbit**  
 Posts: 86  
 Joined: August 19th, 2013, 4:20 pm

**Re: Block internet access for an IP**  
 by **bloater99** » October 17th, 2014, 9:37 pm

Here are the details of my setting:

- Create new rule
- Source: Source address (IP or MAC address for machine)
- leave NAT box unchecked
- Destination: standard network (red)
- Protocol: ALL
- Select Drop radio button
- under Additional settings, check Activate Rule and optionally Log Rule
- click Update. It will return you to main Firewall Rules page
- click Apply Changes
- Rule will show under Firewall Rules. Make sure Activate Rule check box has a check in it.

I hope you can get it working. Double check the machine IP and possibly try the MAC address in its place.

**bloater99**  
 Posts: 482  
 Joined: October 13th, 2014, 3:47 pm



**Re: Block internet access for an IP**  
 by **trymes** » October 17th, 2014, 9:43 pm

Also, as mentioned before, ensure that you do not have another rule above this one that will allow access. The firewall starts at the first rule and compares each packet to see if it matches that rule. It keeps going down the list of rules until one matches, so if another rule matches that packet first, it will never get to the blocking rule you added.

Also, as always, double check for typos in the address, etc. Post up a few screenshots if you are not able to make it work.

Tom

**trymes**  
 Posts: 664  
 Joined: February 9th, 2011, 4:10 pm  
 Location: New England, USA

**Re: Block internet access for an IP**  
 by **catbit** » October 17th, 2014, 10:39 pm

bloater99, trymes

That exactly what I did, I redo the rule even, with the same result.

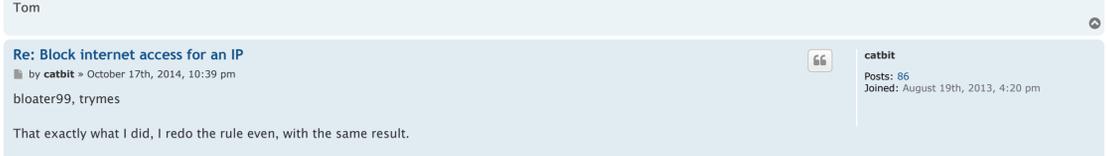
I post a capture.

**catbit**  
 Posts: 86  
 Joined: August 19th, 2013, 4:20 pm

**Re: Block internet access for an IP**  
 by **BeBiMa** » October 18th, 2014, 8:40 am

There are some rules above the first rule. Most important for this problem is the contrack chain. All established connections are accepted before your blocking rules. That means for these connections the rule isn't relevant, it isn't checked.

Is the rule effective after a reboot of IPFire?



**Re: Block internet access for an IP**  
 by **catbit** » October 18th, 2014, 12:41 pm

BeBiMa, after a reboot is the same, the notebook with the "blocked" IP still has internet access.

I'm using core 85, and this is a test what I'm doing, but the idea is to see how to proceed in case if I need block some users.

Where can I see the rules that iptables read when start or restart?

Thanks.

**catbit**  
 Posts: 86  
 Joined: August 19th, 2013, 4:20 pm

**Re: Block internet access for an IP**  
 by **trymes** » October 18th, 2014, 12:50 pm

Core 85? Either that's a typo, or you are using a beta version from the testing branch. You should revert back to Core 84.

To see the IPTable rules, you can log in via SSH or there is a menu item to see them.

Tom

**trymes**  
 Posts: 664  
 Joined: February 9th, 2011, 4:10 pm  
 Location: New England, USA

**Re: Block internet access for an IP**  
 by **catbit** » October 18th, 2014, 12:58 pm

If I'm not wrong iptables -L is the command, right?

I think that there is a file where the rules are stored, or maybe I'm confused with another linux system.

The capture shows my system info.

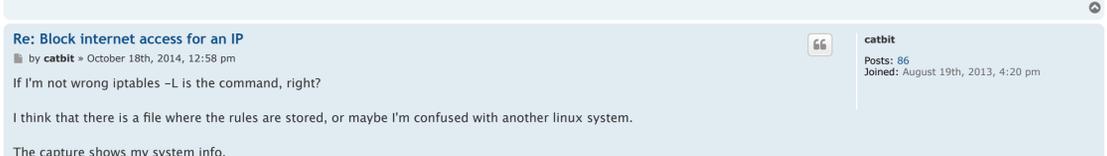
**catbit**  
 Posts: 86  
 Joined: August 19th, 2013, 4:20 pm

**Re: Block internet access for an IP**  
 by **BeBiMa** » October 18th, 2014, 1:14 pm

I just tried.  
 You are right with your expectation.

But I found the reason, also. Do you have activated the proxy? In that case, the requests are not forwarded to the RED interface but sent to the proxy. IPFire's traffic is not blocked in your system, i suppose.  
 You should deny this host in the proxy settings also.  
 ( I tried to send this post, using that proxy blocking )

Last edited by **BeBiMa** on October 18th, 2014, 1:16 pm, edited 1 time in total.

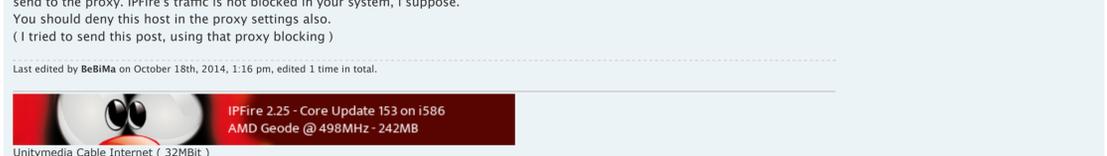


**Re: Block internet access for an IP**  
 by **catbit** » October 18th, 2014, 1:31 pm

No BeBiMa, I'm not using proxy (web proxy).

The notebook connects to internet via wifi, but I have installed Tor plugin, I think that shouldn't be the problem, because in the browser I switch that on or off.

**BeBiMa**  
 Posts: 2842  
 Joined: July 30th, 2011, 12:55 pm  
 Location: Mannheim



**Re: Block internet access for an IP**  
 by **catbit** » October 18th, 2014, 1:31 pm

No BeBiMa, I'm not using proxy (web proxy).

The notebook connects to internet via wifi, but I have installed Tor plugin, I think that shouldn't be the problem, because in the browser I switch that on or off.

**catbit**  
 Posts: 86  
 Joined: August 19th, 2013, 4:20 pm

**Post Reply**

28 posts [1](#) [2](#) [>](#)

Block internet access for an IP

**Re: Block internet access for an IP**  
 by **catbit** » October 18th, 2014, 1:34 pm

bloater99, do you have Tor installed in your ipfire?

**Re: Block internet access for an IP**  
 by **bloater99** » October 20th, 2014, 4:49 pm

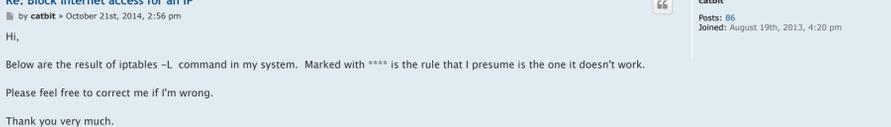
**catbit** wrote:  
 bloater99, do you have Tor installed in your ipfire?

No, I do not. Sorry. You did try using the MAC address in place of the machine IP?



**Re: Block internet access for an IP**  
 by **bloater99** » October 20th, 2014, 4:58 pm

BTW, I now notice that my firewall logs are compromised mostly of blocks to/from this IP. Most of the IPs are from our A/V vendor (even though definitions are set to update from within the LAN) and Akamai Technologies. It is an un-manned PC that is used as a backup server.



**Re: Block internet access for an IP**  
 by **catbit** » October 20th, 2014, 8:14 pm

No, I only tried with IP, but it would be fine to try what you say.

Update: I tried with mac address as source and RED as destination, with the same result. It can not block internet access.

I don't know what happen, what I'm doing wrong.

Last edited by **catbit** on October 20th, 2014, 8:31 pm, edited 1 time in total.

**Re: Block internet access for an IP**  
 by **catbit** » October 21st, 2014, 2:56 pm

Hi,

Below are the result of iptables -L command in my system. Marked with \*\*\*\* is the rule that I presume is the one it doesn't work.

Please feel free to correct me if I'm wrong.

Thank you very much.

```

Chain INPUT (policy DROP)
target prot opt source destination
BADTCP tcp -- anywhere anywhere
CUSTOMINPUT all -- anywhere anywhere
GUARDIAN all -- anywhere anywhere
OVPNBLOCK all -- anywhere anywhere
IPTVINP all -- anywhere anywhere
ICMPINPUT all -- anywhere anywhere
LOOPBACK all -- anywhere anywhere
CONNTRACK all -- anywhere anywhere
DHCPGREENINPUT all -- anywhere anywhere
IPSECINPUT all -- anywhere anywhere
GUININPUT all -- anywhere anywhere
WIRELESSINPUT all -- anywhere anywhere ctstate NEW
OVPNINPUT all -- anywhere anywhere
TOR_INPUT all -- anywhere anywhere
INLPTFW all -- anywhere anywhere
REDINPUT all -- anywhere anywhere
POLICYIN all -- anywhere anywhere

Chain FORWARD (policy DROP)
target prot opt source destination
BADTCP tcp -- anywhere anywhere
TCPMSS tcp -- anywhere anywhere tcp flags:SYN,RST/SYN TCPMSS clamp to PMTU
CUSTOMFORWARD all -- anywhere anywhere
GUARDIAN all -- anywhere anywhere
OVPNBLOCK all -- anywhere anywhere
IPTVFORWARD all -- anywhere anywhere
LOOPBACK all -- anywhere anywhere
CONNTRACK all -- anywhere anywhere
IPSECFORWARD all -- anywhere anywhere
WIRELESSFORWARD all -- anywhere anywhere ctstate NEW
FORWARD all -- anywhere anywhere
UPNPFWD all -- anywhere anywhere ctstate NEW
REDFORWARD all -- anywhere anywhere
POLICYFWD all -- anywhere anywhere

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
CUSTOMOUTPUT all -- anywhere anywhere
LOOPBACK all -- anywhere anywhere
CONNTRACK all -- anywhere anywhere
DHCPGREENOUTPUT all -- anywhere anywhere
IPSECOUTPUT all -- anywhere anywhere
OUTGOINGFW all -- anywhere anywhere
POLICYOUT all -- anywhere anywhere

Chain BADTCP (2 references)
target prot opt source destination
RETURN all -- anywhere anywhere
PSCAN tcp -- anywhere anywhere tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN,PSH,URG
PSCAN tcp -- anywhere anywhere tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN,SYN,RST,ACK,URG
PSCAN tcp -- anywhere anywhere tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN,SYN,RST,PSH,ACK,URG
PSCAN tcp -- anywhere anywhere tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN
PSCAN tcp -- anywhere anywhere tcp flags:SYN,RST/SYN,RST
PSCAN tcp -- anywhere anywhere tcp flags:FIN,SYN/FIN,SYN
PSCAN tcp -- anywhere anywhere tcp flags:FIN,SYN,RST,PSH,ACK,URG/NONE
NEWNOTSYN tcp -- anywhere anywhere tcp flags:!FIN,SYN,RST,ACK/SYN ctstate NEW

Chain CONNTRACK (3 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
DROP all -- anywhere anywhere ctstate INVALID

Chain CUSTOMFORWARD (1 references)
target prot opt source destination

Chain CUSTOMINPUT (1 references)
target prot opt source destination

Chain CUSTOMOUTPUT (1 references)
target prot opt source destination

Chain DHCPBLUEINPUT (0 references)
target prot opt source destination

Chain DHCPBLUEOUTPUT (0 references)
target prot opt source destination

Chain DHCPGREENINPUT (1 references)
target prot opt source destination
DHCPINPUT all -- anywhere anywhere

Chain DHCPGREENOUTPUT (1 references)
target prot opt source destination
DHCPOUTPUT all -- anywhere anywhere

Chain DHCPINPUT (1 references)
target prot opt source destination
ACCEPT udp -- anywhere anywhere udp spt:bootpc dpt:bootps
ACCEPT tcp -- anywhere anywhere tcp spt:bootpc dpt:bootps

Chain DHCPOUTPUT (1 references)
target prot opt source destination
ACCEPT udp -- anywhere anywhere udp spt:bootps dpt:bootpc
ACCEPT tcp -- anywhere anywhere tcp spt:bootps dpt:bootpc

Chain FORWARDFW (1 references)
target prot opt source destination
DROP all -- anywhere anywhere MAC 00:26:C7:99:AA:FC **** This is the rule ****
ACCEPT udp -- anywhere anywhere 172.16.0.250 udp dpts:lua:dnp
ACCEPT tcp -- anywhere anywhere garage tcp dpt:51414
ACCEPT tcp -- anywhere anywhere garage tcp dpt:51413
ACCEPT udp -- anywhere anywhere 172.16.0.250 udp dpt:slp
DROP all -- anywhere anywhere ip2p v0.8.2-ipfire --kazaa --gnu --edk --dc --apple --soul --winmx --ares

Chain GUARDIAN (2 references)
target prot opt source destination

Chain GUININPUT (1 references)
target prot opt source destination
ACCEPT tcp -- anywhere anywhere tcp dpt:snpp

Chain ICMPINPUT (1 references)
target prot opt source destination
ACCEPT icmp -- anywhere anywhere icmp echo-request

Chain INPUTFW (1 references)
target prot opt source destination
ACCEPT tcp -- anywhere anywhere 190.8.92.142 tcp dpt:7699

Chain IPSECFORWARD (1 references)
target prot opt source destination

Chain IPSECINPUT (1 references)
target prot opt source destination

Chain IPSECOUTPUT (1 references)
target prot opt source destination

Chain IPTVFORWARD (1 references)
target prot opt source destination

Chain IPTVINPUT (1 references)
target prot opt source destination

Chain LOG_DROP (0 references)
target prot opt source destination
LOG all -- anywhere anywhere limit: avg 10/min burst 5 LOG level warning
DROP all -- anywhere anywhere

Chain LOG_REJECT (0 references)
target prot opt source destination
LOG all -- anywhere anywhere limit: avg 10/min burst 5 LOG level warning
REJECT all -- anywhere anywhere reject-with icmp-port-unreachable

Chain LOOPBACK (3 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere
ACCEPT all -- anywhere anywhere
DROP all -- 127.0.0.0/8
DROP all -- anywhere 127.0.0.0/8

Chain NEWNOTSYN (1 references)
target prot opt source destination
LOG all -- anywhere anywhere limit: avg 10/min burst 5 LOG level warning prefix "DROP_NEWNOTSYN "
DROP all -- anywhere anywhere /* DROP_NEWNOTSYN */

Chain OUTGOINGFW (1 references)
target prot opt source destination

Chain OVPNBLOCK (3 references)
target prot opt source destination

Chain OVPNINPUT (1 references)
target prot opt source destination

Chain POLICYFWD (1 references)
target prot opt source destination
ACCEPT all -- 172.16.0.0/24 anywhere
ACCEPT all -- anywhere anywhere policy match dir in pol ipsec
ACCEPT all -- anywhere anywhere
ACCEPT all -- 172.16.1.0/24 anywhere
LOG all -- anywhere anywhere limit: avg 10/min burst 5 LOG level warning prefix "DROP_FORWARD "
DROP all -- anywhere anywhere /* DROP_FORWARD */

Chain POLICYIN (1 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere
ACCEPT all -- anywhere anywhere policy match dir in pol ipsec
ACCEPT all -- anywhere anywhere
LOG all -- anywhere anywhere limit: avg 10/min burst 5 LOG level warning prefix "DROP_INPUT "
DROP all -- anywhere anywhere /* DROP_INPUT */

Chain POLICYOUT (1 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere
DROP all -- anywhere anywhere /* DROP_OUTPUT */

Chain PSCAN (7 references)
target prot opt source destination
LOG tcp -- anywhere anywhere limit: avg 10/min burst 5 /* DROP_TCP PSCAN */ LOG level warning prefix
"DROP_TCP Scan "
LOG udp -- anywhere anywhere limit: avg 10/min burst 5 /* DROP_UDP PSCAN */ LOG level warning prefix
"DROP_UDP Scan "
LOG icmp -- anywhere anywhere limit: avg 10/min burst 5 /* DROP_ICMP PSCAN */ LOG level warning prefix
"DROP_ICMP Scan "
LOG all -f anywhere anywhere limit: avg 10/min burst 5 /* DROP_FRAG PSCAN */ LOG level warning prefix
"DROP_FRAG Scan "
DROP all -- anywhere anywhere /* DROP_PSCAN */

Chain REDFORWARD (1 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere

Chain REDINPUT (1 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere

Chain TOR_INPUT (1 references)
target prot opt source destination

Chain UPNPFWD (1 references)
target prot opt source destination

Chain WIRELESSFORWARD (1 references)
target prot opt source destination

Chain WIRELESSINPUT (1 references)
target prot opt source destination
    
```

**Re: Block internet access for an IP**  
 by **catbit** » October 29th, 2014, 3:23 pm

Sadly, it seems that any rule I test is destined to fail. It seems simple but in fact I cannot make this work for me, maybe my system has a bug, a reinstall could be a solution, I don't know.

Even a scheduled task failed, something is wrong with my ipfire.

cheers. 😊

**Re: Block internet access for an IP**  
 by **trymes** » October 29th, 2014, 3:34 pm

Catbit: Post a screenshot of the rule configuration page. That might clear up why it is not working.

Tom

**Re: Block internet access for an IP**  
 by **catbit** » October 29th, 2014, 4:19 pm

Thank you trymes,

This screenshot is the same I posted October 18. This is the rule that doesn't work even rebooting the system.

UPDATE: after a clean reinstall of core 85, the rule exposed in this post worked correctly. It seems that a failed update or something else were the cause of the malfunction.

Last edited by **catbit** on November 19th, 2014, 9:47 pm, edited 1 time in total.

**Re: Block internet access for an IP**  
 by **emsi** » October 30th, 2014, 1:18 am

Hi, how can I block internet access of group of computers in easiest way using IPFire. The IP address of the computers to block is from 192.168.0.20 to 192.168.0.80.

Then computers with internet access are 192.168.100 to 192.168.0.20

Thank you. 😊 😊 😊 😊

I have read in this forum that I can use firewall rule to block it, can you enumerate to me how that can be done.. thanks again

What firewall mode should I choose 0,1 or 2? I'm sorry I'm still newbie in ipfire.

**Re: Block internet access for an IP**  
 by **trymes** » October 30th, 2014, 1:25 am

Well, you might be best served by starting a new thread. Having said that, your IP addresses above are incomplete, but the way you would do this is to define the address range in the "Firewall Groups" section of the interface, and then craft a rule for that group.

However, you asked about which mode to use, which means that you likely are running an older version of IPFire that doesn't have the Groups functionality. What version are you running?

Tom

**Re: Block internet access for an IP**  
 by **bloater99** » October 30th, 2014, 4:24 pm

**emsi** wrote:  
 Hi, how can I block internet access of group of computers in easiest way using IPFire. The IP address of the computers to block is from 192.168.0.20 to 192.168.0.80.  
 Then computers with internet access are 192.168.100 to 192.168.0.20

I have read in this forum that I can use firewall rule to block it, can you enumerate to me how that can be done.. thanks again

What firewall mode should I choose 0,1 or 2? I'm sorry I'm still newbie in ipfire.

Here's how I did it:  
 Firewall -> Firewall Groups  
 click Hosts button  
 under Add New Host, type a descriptive name, IP/MAC address for that machine and an optional remark, then click Save. I don't think you can do ranges, I tried that at first and could not get it to work. So you put individual hosts in (each with their IP/MAC). You will soon have a list of hosts showing at the bottom of the page.  
 Now you click on Network/Host Groups button.  
 Type a group name and optional remark and click Add button.  
 You will now see the group name below the Network/Host Groups heading.  
 Click on the pencil icon to the right of the group name to Edit.  
 you will see your group name under Add new network/host group.  
 Click on the Hosts radio button, in the dropdown menu to the right of it, click each Host name, then click the Add button. When you are done, you will see each machine in the group list at the bottom of the page (mine is highlighted in yellow)

Now when you go to Firewall Rules, next to the Network/hosts group radio button, you will see your group name as an option under Source.

It is a bit clunky. Maybe there's a better way, but that's how I did it, and it does work for me.



**Re: Block internet access for an IP**  
 by **trymes** » October 30th, 2014, 5:11 pm

You can add a range of IPs by using subnet notation. Google a subnet calculator and you should be able to figure out the proper notation to achieve what you want.

**Re: Block internet access for an IP**  
 by **emsi** » October 31st, 2014, 8:09 am

**trymes** wrote:  
 Well, you might be best served by starting a new thread. Having said that, your IP addresses above are incomplete, but the way you would do this is to define the address range in the "Firewall Groups" section of the interface, and then craft a rule for that group.

However, you asked about which mode to use, which means that you likely are running an older version of IPFire that doesn't have the Groups functionality. What version are you running?

Tom

I actually started a forum 3 days ago regarding this matter but only 1 person replied. I am using version 2.13 but I will be trying to install the newer version.

This is the link to my own thread, <http://forum.ipfire.org/viewtopic.php?t=0> you can also reply there if you don't mind thanks