

# Re: Determining what should be blocked in and out?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2001-12/1656.html>

---

**From:** sponge ([mtubi@python.net](mailto:mtubi@python.net))

**Date:** 12/27/01

From: [mtubi@python.net](mailto:mtubi@python.net) (sponge)

Date: Thu, 27 Dec 2001 05:13:46 GMT

On Wed, 19 Dec 2001 16:57:34 +0200, Lance Delacroix

<[lance\\_delacroix@fastmail.fm](mailto:lance_delacroix@fastmail.fm)> wrote:

>On 19 Dec 2001 10:23:01 GMT, [eirik@peter.mi.uib.no](mailto:eirik@peter.mi.uib.no) (Eirik Seim) wrote:

>

>>On Wed, 19 Dec 2001 09:46:51 +0200, Lance Delacroix

>> <[lance\\_delacroix@fastmail.fm](mailto:lance_delacroix@fastmail.fm)> wrote:

>>>Great post -- thanks! I need some clarification, though, on a couple  
>>>of points.

>>>

>>>

>>>On Wed, 19 Dec 2001 04:29:22 GMT, [mtubi@python.net](mailto:mtubi@python.net) (sponge) wrote:

>>>

>>>>208.184.172.0 (the /24 means the first three dotted numbers must be

>>>>entered as shown; you add a dot and a zero. If it says /16, only the

>>>>first two dotted numbers should be added (you add a .0 and again a .0)

>>>>

>>>>I'm confused by this /24 and /16. You simply mean that you

>>>>substitute .0 for /24 and you substitute .0.0 for /16?

>>>>

>>>>Sort of, yes. But I think it is somewhat important to know *\_why\_*, making

>>>>it easier to block certain IP ranges yourself. Read on.

>>>>

>>>>>Note: Alexa may use all of 209.247/16. Play it safe and block the

>>>>>whole thing (209.247.0.0-209.247.255.255)

>>>>>

>>>>>Here you have a range shown. Do you enter the range exactly as

>>>>>shown, or does each individual IP address need its own rule?

>>>>>

>>>>>I don't know about the product you're using, but it should be able to

>>>>>understand simply 209.247/16.

>>>>>

>>>>>Tiny Personal Firewall, and it doesn't like that format at all.

>>>>>

>>>>>Check out <http://public.pacbell.net/dedicated/cidr.html> if I don't make any

## comp.security.firewalls: Re: Determining what should be blocked in and out?

>>sense. I've not even finished my first coffe yet :)  
>  
>You do make sense, and you also show me my own ignorance. One more  
>question: Does using an address that ends in 0. or 0.0. automatically  
>specify a range?

Usually, but not always. For what we're doing, it's good enough. It depends upon the exact context, but, yes, usually. If I want to block, say, the entire chunk of Class C IPs owned by Alexa, I just put in 209.247.41.0 and then in TPF's Mask block put in 255.255.255.0. What will happen is that the firewall will do a logical AND of any IP addresses coming through it and 255.255.255.0. The last byte of the mask, the .0, will always make the last byte of the IP address you're checking 0. Since the reference address (209.247.41.0) also has the last byte as 0, that means the last byte doesn't matter and it will be zero always for the purposes of checking if it's to be blocked. If the first three bytes of the IP being checked match the network (which you specified in TPF with the first three bytes—in this case, 209.247.41), it will be blocked. In other words, the mask filters out the variable part (the range to be blocked, in this case, 256 possible host addresses, or 209.247.41.0 to 209.247.41.255). With a /16 (or a Class B) you use a mask of 255.255.0.0 and that will set the last TWO bytes to zero.

However, you could get creative and want to block, say, 209.247.41.192 to 209.247.41.255. To do this (209.247.41.192/26) you would put 209.247.41.192 in the netblock box. That 192 makes the first two bits of the last byte ones. You also would use a mask of 255.255.255.192. This makes sure the first two bits of the last byte are set in the mask so proper checking can be done and you don't block too much or too little. The ANDing process will assure that any IP address being checked will have the last 6 bits set to zero before checking against the netblock (whose last six bits are also zero.)

The reason why this is necessary is because, nowadays, more and more networks are being "split up". It used to be that a company had to buy IP addresses in chunks of 256 (in the case of Class Cs) or 65,536 (for Class Bs.) Because IPs have become such a precious commodity, they are often split, especially amongst Class Bs. So, if you own one of these, you need CIDR notation to be able to work at the bit level in order to determine which networks are yours and which ones are someone elses.

The blocking method is used by your own computer to determine if an IP address you are trying to contact is on the same network as you. It is extremely fast. Every packet which communicates with another machine is ANDed in a similar manner. The reason why is your computer needs to know if each packet of data needs to be sent out onto the Internet or if it's good enough to simply send it locally.

That's why I wrote this the way I did. It is much, much faster to use TPF's net blocking method than to block a "range" of IP addresses, because this method requires very little CPU time. Blocking by range, on the other hand, requires the firewall to figure out if an IP being checked is less than this this number or more than that number, etc.

However, I think I will revise this to specify a range and keep the

comp.security.firewalls: Re: Determining what should be blocked in and out?

instructions the same. I had a feeling the CIDR notation might throw people.

Examples:

Network being blocked 209.247.41/24 (209.247.41.0)

Mask: 255.255.255.0

IP address to be checked: 209.247.41.36

IP 11010001 . 11110111 . 00101001 . 00100100 (209.247.41.36)

Mask 11111111 . 11111111 . 11111111 . 00000000 (255.255.255.0)

Equals 11010001 . 11110111 . 00101001 . 00000000 (209.247.41.0)

Since this equals the network to be blocked, it will be blocked.

Network being blocked 209.247.41.192/26

Mask: 255.255.255.192

IP address to be checked: 209.247.41.193

IP 11010001 . 11110111 . 00101001 . 11000010 (209.247.41.194)

Mask 11111111 . 11111111 . 11111111 . 11000000 (255.255.255.192)

Equals 11010001 . 11110111 . 00101001 . 11000000 (209.247.41.192)

Since this equals the same network to be blocked, it will be blocked.

Network being blocked 209.247/16 (209.247.0.0–209.247.255.255)

Mask 255.255.0.0

IP address to be checked: 209.247.13.3

IP 11010001 . 11110111 . 00001101 . 00000011 (209.247.13.3)

Mask 11111111 . 11111111 . 00000000 . 00000000 (255.255.0.0)

Equals 11010001 . 11110111 . 00000000 . 00000000 (209.247.0.0)

Since this equals 209.247 (don't care what the other two bytes are)

it will be blocked.

>Thanks!

- 
- **Next message:** [sponge: "Re: HEY, SPONGE / here is Gator IP"](#)
  - **Previous message:** [George Wenzel: "Re: Outpost Email problem"](#)
  - **In reply to:** [Lance Delacroix: "Re: Determining what should be blocked in and out?"](#)
  - **Next in thread:** [Lance Delacroix: "Re: Determining what should be blocked in and out?"](#)
  - **Next in thread:** [Dr. Bob: "Re: Determining what should be blocked in and out?"](#)
  - **Reply:** [Lance Delacroix: "Re: Determining what should be blocked in and out?"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)