

## Introduction

Too many firewall administrators continue to deploy firewall policies with the object ‘Any’ being used as either the source or destination for Internet access rules. The Internet is not ‘Any’ and it should never be conflated in that way. Conflating “Any” with “The Internet” provides much more access than is actually required and may give access to sources or destinations that were never intended. This document provides information and guidance to help to eliminate this common misconception and malpractice.

## ‘The Internet’ is NOT ‘Any’

Time after time, policy rules are implemented on firewalls that are intended to allow access to or from the Internet where the corresponding destination or source object is set to ‘Any’. The object ‘Any’ (which is all of the IPv4 address space from 0.0.0.0 to 255.255.255.255) includes much, much more than just the official Internet address space – and this is a problem. In fact, the ‘Any’ object applies to all DMZ’s on the firewall where ‘Any’ is configured. Granted, many firewalls use zoning schemes that block traffic from within one zone from reaching other zones that have a higher or different security rating or name. But that is not the case for many, many other firewalls and even for those that do have zoning restrictions, those restrictions can be reconfigured or disabled entirely. Furthermore, changes in zoning, NATing or routing can alter the scope of reach for rules that use “Any”. As a result, the use of ‘Any’ as the equivalent of ‘the Internet’ is likely to allow access to or from zones that was never actually intended and may alter the scope of reachable networks if changes are made to the firewall. This breaks the first law of good firewall security policy – ***“thou shalt give access only to that which is required”***. **Firewall rules that are intended to allow access to or from “The Internet” should use a group object to limit the scope of the rule so that access is explicitly restricted to the address space of the Internet itself.** This ‘The Internet’ object must exclude all address space that is explicitly NEVER a part of the routable Internet address space. Furthermore, this ‘The Internet’ group object should only contain network address space that is NOT a part of any other zone on the firewall where the object will be used. This would ensure that no other zone can be accessed via a rule that uses the Internet group object. Creating multiple Internet group objects can be a challenge especially when a central database is used for managing multiple firewalls. Let us look at ways to define the Internet group object.

## The Internet is NOT RFC-5735

[RFC-5735](#) provides a short list of networks that are definitely NOT a part of the Internet IPv4 address space. This RFC provides the starting point for defining what the Internet actually is NOT. From that baseline it is possible to reverse extrapolate what the routable Internet address space actually IS. The [Appendix I](#) contain several different definitions for the Internet based upon this strict approach.

Using a ‘The Internet’ group object that is defined based upon these criteria is a significant improvement over the very sub optimal ‘Any’. We encourage all firewall administrators to implement a ‘The Internet’ object using this approach **as an absolute bare minimum**. In other words, ‘Any’ should be replaced with “The Internet” group object wherever possible. NOTE: The circumstances that require the use of ‘Any’ are extremely rare in a firewall policy. Even when a scanning device (EG: Qualys, Nessus) requires access to all DMZ’s, the rule should allowing scanning access to all subnets can use a “ALL DMZ subnets” group instead of ‘Any’. See the document “Thou shalt not use ANY” for additional details on why ANY should not be used and methods for avoiding its use.

## Bogons

The Internet object we have thus far discussed contains all of the routable IPv4 address space that can exist on the Internet. However, significant portions of that space will not be in use at all times. Even though the vast majority of IPv4 address space that can be used on the Internet has been allocated; there are still many large and small blocks of address space that will not be in use at any particular point in time. Blocks of Internet routable address space that are not currently in operational use on the Internet are known as ‘bogons’. In the past, there were significant benefits to be had by blocking or dropping bogons because a large percentage of bogus traffic (often nefarious) would originate using bogon addresses. However, the effort required to maintain an accurate and up to date firewall group object that excludes all bogons is significant. Daily efforts are required. A far better approach is to block bogons using routing devices and to automate the process. If your organization uses Internet edge routers then setting up black hole routing of bogon subnets is highly desirable. [Team Cymru](#) provides a free service that can be used to automatically drop bogon traffic by setting up peering between your Internet BGP capable routers and the Team Cymru BGP routers that maintain a day to day accurate list of bogons. A further enhancement would be to advertise the bogons that you receive from Team Cymru and inject them into your upstream service provider’s network edge using special BGP communities (if the ISP provides this service). This method drops bogon traffic at your ISP edge which has the distinct advantage of dropping bogon traffic before it even enters your upstream ISP connection. Since bogon traffic is significantly less than what it used to be we do not believe that attempting to maintain the firewall Internet group object to exclude bogons is worthwhile. However, we do recommend setting up bogon dropping automation on your Internet edge routers. Setting up such automation also allows leveraging of similar black hole techniques for blocking of nefarious hosts at your Internet edge routers (or upstream ISP connections) too. See the document “Thou shall automate blackholing” for details.

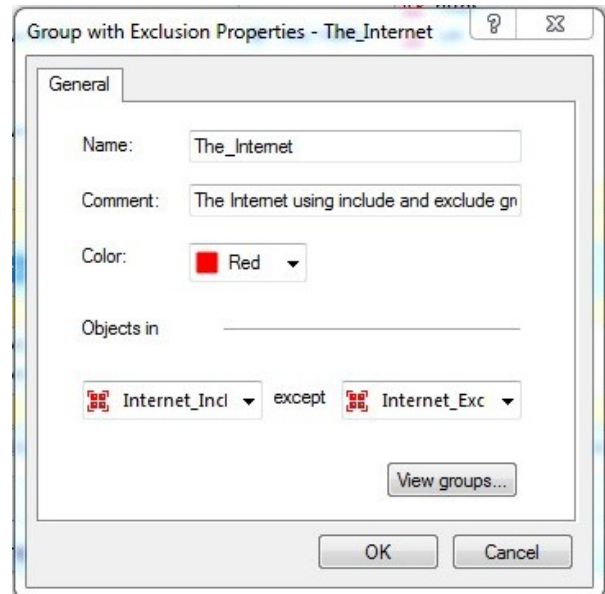
## Private Network Connections

The Internet object we have thus far discussed contains all of the Internet routable address space and might exclude bogons. But we are not yet finished because in many cases, third parties that your

organization may be connected to will be utilizing IPv4 address space that was allocated to them from the Internet address space. Your organization will often connect to those third parties via private network services. In many if not most cases, the private connections will be attached to your firewalls via zones that are not connected to the Internet zone (the zone that is often called ‘external’). That is, the private connections will attach to your network via a different DMZ from your Internet zone attachment. They may even connect to your organization via a completely different firewall and your organization may route these subnets in your internal network. In any case, ‘The Internet’ group object (discussed so far) would contain address space that exists on a different zone on your firewall. It would be highly optimal to exclude such third party address space from your Internet object. However, removing those subnets that exist on other zones requires reanalyzing the address space and editing the Internet subnet list such that third party ranges are removed. A trade off might be to accept that third parties shall be treated as though they are indeed a part of the Internet. Each organization must assess the security implications of either approach and must determine if the trade off in security is acceptable or if the additional work effort that is required to maintain the Internet object including these special exclusions is worthwhile. Automation (through the use of scripts) is highly desirable. Using scripts allows for the collection of routing tables from firewalls and routers. The scripts can also carry out the required analysis and creation of the lists of subnets that represent the Internet.

## The Check Point “The\_Internet” Group

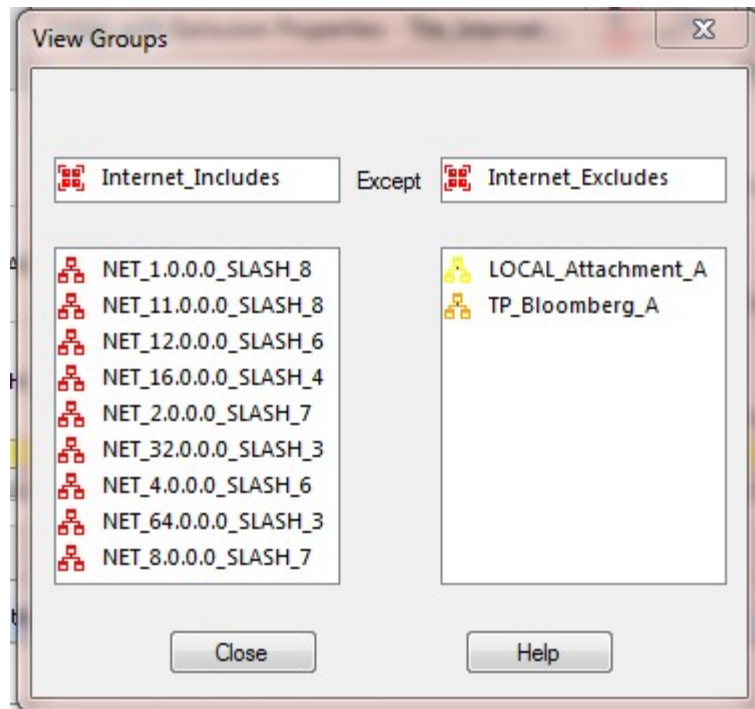
The Check Point firewall objects database can include a group defined to be “The\_Internet” that is of type “Group With Exclusion”. This group would use two sub groups called “Internet\_Inclusive” and “Internet\_Exclusive”. These two groups define those network addresses that are to be included in the scope and those that are to be excluded. This has the effect of ensuring that access provisioned from “The\_Internet” to hosts and services will not include other segregated zones or internal networks ETC. The screen capture at right shows the “Group With Exclusion” type.



The screen capture below (next page) shows an example of the content of both groups. The content of the inclusive group object shows that individual network objects have been created that represent the officially routable Internet address space (using the subnets listed in this section below). And, all of those network objects have been added to the ‘Internet\_Includes’ group object. In addition, any

address space that would normally be routable on the Internet but is being used on other zones or locally attached have been defined and added to the ‘Internet\_Excludes’ exclusion group.

The exclusion group should include all specific address ranges that are internal or segregated that are also Internet routable. This can and should include any Internet address space that the CLIENT may be routing via other zones (such as other third parties that use their Internet registered address space in their private networks to which your network is attached), as well as various Internet attachment subnets and IP addresses and other IP address space that may be in use internally. Note that it is not necessary to add RFC-1918 or other address space to the exclusion group since it is not included in the inclusion group in the first place.



This method of maintaining “The Internet” object allows for simple maintenance because the inclusion group is static and never changes (unless IANA changes it’s official use of IPv4 address space which is extremely rare and even more unlikely at this late stage in the IPv4 life cycle).

**IMPORTANT:** Directly connected local Internet attachment subnets (such as a used by CLIENT routers and other external devices) and CLIENT Internet presented host IP’s, NAT’s etc should NOT be included in the Internet group. If there is a requirement to permit external CLIENT IP’s to reach CLIENT hosts and services then a separate group shall be created that contains such external CLIENT IP address, subnets and or ranges. Such a group shall be named CLIENT\_External\_xxx, and shall be representative of location and or other identifying information.

## The Internet CIDR List

The following list provides the precise subnets that are required to define the officially routable IPv4 Internet address space. (Please always check for errors and omissions). This list may be used to create the required network objects that become the officially routable Internet object for use in your firewall policies. The list below gives the subnet in CIDR notation followed by the equivalent subnet mask.



1.0.0.0/8-255.0.0.0  
2.0.0.0/7-254.0.0.0  
4.0.0.0/6-252.0.0.0  
8.0.0.0/7-254.0.0.0  
11.0.0.0/8-255.0.0.0  
12.0.0.0/6-252.0.0.0  
16.0.0.0/4-240.0.0.0  
32.0.0.0/3-224.0.0.0  
64.0.0.0/3-224.0.0.0  
96.0.0.0/4-240.0.0.0  
112.0.0.0/5-248.0.0.0  
120.0.0.0/6-252.0.0.0  
124.0.0.0/7-254.0.0.0  
126.0.0.0/8-255.0.0.0  
128.0.0.0/3-224.0.0.0  
160.0.0.0/5-248.0.0.0  
168.0.0.0/8-255.0.0.0  
169.0.0.0/9-255.128.0.0  
169.128.0.0/10-255.192.0.0  
169.192.0.0/11-255.224.0.0  
169.224.0.0/12-255.240.0.0  
169.240.0.0/13-255.248.0.0  
169.248.0.0/14-255.252.0.0  
169.252.0.0/15-255.254.0.0  
169.255.0.0/16-255.255.0.0  
170.0.0.0/7-254.0.0.0  
**172.0.0.0/12-255.240.0.0**  
172.32.0.0/11-255.224.0.0  
172.64.0.0/10-255.192.0.0  
172.128.0.0/9-255.128.0.0  
173.0.0.0/8-255.0.0.0  
174.0.0.0/7-254.0.0.0  
176.0.0.0/4-240.0.0.0  
192.0.1.0/24-255.255.255.0  
192.0.3.0/24-255.255.255.0  
192.0.4.0/22-255.255.252.0  
192.0.8.0/21-255.255.248.0  
192.0.16.0/20-255.255.240.0  
192.0.32.0/19-255.255.224.0  
192.0.64.0/18-255.255.192.0  
192.0.128.0/17-255.255.128.0  
192.1.0.0/16-255.255.0.0  
192.2.0.0/15-255.254.0.0  
192.4.0.0/14-255.252.0.0  
**192.8.0.0/13-255.248.0.0**  
192.16.0.0/12-255.240.0.0  
192.32.0.0/11-255.224.0.0  
192.64.0.0/12-255.240.0.0  
192.80.0.0/13-255.248.0.0  
192.88.0.0/18-255.255.192.0  
192.88.64.0/19-255.255.224.0  
192.88.96.0/23-255.255.254.0



192.88.98.0/24-255.255.255.0  
192.88.100.0/22-255.255.252.0  
192.88.104.0/21-255.255.248.0  
192.88.112.0/20-255.255.240.0  
192.88.128.0/17-255.255.128.0  
192.89.0.0/16-255.255.0.0  
192.90.0.0/15-255.254.0.0  
192.92.0.0/14-255.252.0.0  
192.96.0.0/11-255.224.0.0  
192.128.0.0/11-255.224.0.0  
192.160.0.0/13-255.248.0.0  
192.169.0.0/16-255.255.0.0  
192.170.0.0/15-255.254.0.0  
192.172.0.0/14-255.252.0.0  
192.176.0.0/12-255.240.0.0  
192.192.0.0/10-255.192.0.0  
193.0.0.0/8-255.0.0.0  
194.0.0.0/7-254.0.0.0  
196.0.0.0/6-252.0.0.0  
198.0.0.0/12-255.240.0.0  
198.16.0.0/15-255.254.0.0  
198.20.0.0/14-255.252.0.0  
198.24.0.0/13-255.248.0.0  
198.32.0.0/12-255.240.0.0  
198.48.0.0/15-255.254.0.0  
198.50.0.0/16-255.255.0.0  
**198.51.0.0/18-255.255.192.0**  
198.51.64.0/19-255.255.224.0  
198.51.96.0/22-255.255.252.0  
198.51.101.0/24-255.255.255.0  
198.51.102.0/23-255.255.254.0  
198.51.104.0/21-255.255.248.0  
198.51.112.0/20-255.255.240.0  
198.51.128.0/23-255.255.254.0  
198.52.0.0/14-255.252.0.0  
198.56.0.0/13-255.248.0.0  
198.64.0.0/10-255.192.0.0  
198.128.0.0/9-255.128.0.0  
199.0.0.0/8-255.0.0.0  
200.0.0.0/5-248.0.0.0  
208.0.0.0/4-240.0.0.0

## Appendix I

The following information is provided for informational purposes only. We accept no responsibility for any errors, inclusions or omissions. It is recommended that the reader check the information before using it in any capacity whatsoever.

## ***Cisco IOS extended access list that allows any to the Internet***

```
#####  
# Cisco IOS extended access list that allows any to the Internet  
# the list is based upon RFC-5735.  
# See http://tools.ietf.org/html/rfc5735  
#####  
#####  
# Check all of the information below for errors and omissions.  
# The access list includes 'remark deny' statements for networks that  
# are NOT a part of the Internet and includes permit statements for  
# all other IPv4 address space.  
#####  
ip access-list extended TheSimpleInternet  
remark deny ip any 0.0.0.0 0.255.255.255  
permit ip any 1.0.0.0 0.255.255.255  
permit ip any 2.0.0.0 1.255.255.255  
permit ip any 4.0.0.0 3.255.255.255  
permit ip any 8.0.0.0 1.255.255.255  
remark deny ip any 10.0.0.0 0.255.255.255  
permit ip any 11.0.0.0 0.255.255.255  
permit ip any 12.0.0.0 3.255.255.255  
permit ip any 16.0.0.0 15.255.255.255  
permit ip any 32.0.0.0 31.255.255.255  
permit ip any 64.0.0.0 31.255.255.255  
permit ip any 96.0.0.0 15.255.255.255  
permit ip any 112.0.0.0 7.255.255.255  
permit ip any 120.0.0.0 3.255.255.255  
permit ip any 124.0.0.0 1.255.255.255  
permit ip any 126.0.0.0 0.255.255.255  
remark deny ip any 127.0.0.0 0.255.255.255  
permit ip any 128.0.0.0 31.255.255.255  
permit ip any 160.0.0.0 7.255.255.255  
permit ip any 168.0.0.0 0.255.255.255  
permit ip any 169.0.0.0 0.127.255.255  
permit ip any 169.128.0.0 0.63.255.255  
permit ip any 169.192.0.0 0.31.255.255  
permit ip any 169.224.0.0 0.15.255.255  
permit ip any 169.240.0.0 0.7.255.255  
permit ip any 169.248.0.0 0.3.255.255  
permit ip any 169.252.0.0 0.1.255.255  
remark deny ip any 169.254.0.0 0.0.255.255  
permit ip any 169.255.0.0 0.0.255.255  
permit ip any 170.0.0.0 1.255.255.255  
permit ip any 172.0.0.0 0.15.255.255  
remark deny ip any 172.16.0.0 0.15.255.255  
permit ip any 172.32.0.0 0.15.255.255  
permit ip any 172.64.0.0 0.63.255.255  
permit ip any 172.128.0.0 0.127.255.255  
permit ip any 173.0.0.0 0.255.255.255  
permit ip any 174.0.0.0 1.255.255.255  
permit ip any 176.0.0.0 15.255.255.255
```



```
remark deny ip any 192.0.0.0 0.0.0.255
permit ip any 192.0.1.0 0.0.0.255
remark deny ip any 192.0.2.0 0.0.0.255
permit ip any 192.0.3.0 0.0.0.255
permit ip any 192.0.4.0 0.0.3.255
permit ip any 192.0.8.0 0.0.7.255
permit ip any 192.0.16.0 0.0.15.255
permit ip any 192.0.32.0 0.0.31.255
permit ip any 192.0.64.0 0.0.63.255
permit ip any 192.0.128.0 0.0.127.255
permit ip any 192.1.0.0 0.0.255.255
permit ip any 192.2.0.0 0.1.255.255
permit ip any 192.4.0.0 0.3.255.255
permit ip any 192.8.0.0 0.7.255.255
permit ip any 192.16.0.0 0.15.255.255
permit ip any 192.32.0.0 0.31.255.255
permit ip any 192.64.0.0 0.15.255.255
permit ip any 192.80.0.0 0.7.255.255
permit ip any 192.88.0.0 0.0.63.255
permit ip any 192.88.64.0 0.0.31.255
permit ip any 192.88.96.0 0.0.1.255
permit ip any 192.88.98.0 0.0.0.255
remark ip any deny 192.88.99.0 0.0.0.255
permit ip any 192.88.100.0 0.0.3.255
permit ip any 192.88.104.0 0.0.7.255
permit ip any 192.88.112.0 0.0.15.255
permit ip any 192.88.128.0 0.0.127.255
permit ip any 192.89.0.0 0.0.255.255
permit ip any 192.90.0.0 0.1.255.255
permit ip any 192.92.0.0 0.3.255.255
permit ip any 192.96.0.0 0.31.255.255
permit ip any 192.128.0.0 0.31.255.255
permit ip any 192.160.0.0 0.7.255.255
remark deny ip any 192.168.0.0 0.0.255.255
permit ip any 192.169.0.0 0.0.255.255
permit ip any 192.170.0.0 0.1.255.255
permit ip any 192.172.0.0 0.3.255.255
permit ip any 192.176.0.0 0.15.255.255
permit ip any 192.192.0.0 0.63.255.255
permit ip any 193.0.0.0 0.255.255.255
permit ip any 194.0.0.0 1.255.255.255
permit ip any 196.0.0.0 3.255.255.255
permit ip any 198.0.0.0 0.15.255.255
permit ip any 198.16.0.0 0.1.255.255
remark deny any 198.18.0.0 0.1.255.255
permit ip any 198.20.0.0 0.3.255.255
permit ip any 198.24.0.0 0.7.255.255
permit ip any 198.32.0.0 0.15.255.255
permit ip any 198.48.0.0 0.1.255.255
permit ip any 198.50.0.0 0.0.255.255
permit ip any 198.51.0.0 0.0.63.255
permit ip any 198.51.64.0 0.0.31.255
```





```
permit ip any 198.51.96.0 0.0.3.255
remark deny ip any 198.51.100.0 0.0.0.255
permit ip any 198.51.101.0 0.0.0.255
permit ip any 198.51.102.0 0.0.1.255
permit ip any 198.51.104.0 0.0.7.255
permit ip any 198.51.112.0 0.0.15.255
permit ip any 198.51.128.0 0.0.127.255
permit ip any 198.52.0.0 0.3.255.255
permit ip any 198.56.0.0 0.7.255.255
permit ip any 198.64.0.0 0.63.255.255
permit ip any 198.128.0.0 0.127.255.255
permit ip any 199.0.0.0 0.255.255.255
permit ip any 200.0.0.0 7.255.255.255
permit ip any 208.0.0.0 15.255.255.255
remark deny ip any 224.0.0.0 31.255.255.255
remark deny ip any any
#####
```

### Cisco ASA “TheInternet” Object

```
#####
#####
# Cisco ASA group 'TheInternet' is made up of a list of IPv4 network
# objects that are members of group 'TheInternet'
# List is based upon RFC-5735 see http://tools.ietf.org/html/rfc5735
#####
#####
# Check all of the information for errors and omissions.
#####
object network 1.0.0.0-255.0.0.0
subnet 1.0.0.0 255.0.0.0
object network 2.0.0.0-254.0.0.0
subnet 2.0.0.0 254.0.0.0
object network 4.0.0.0-252.0.0.0
subnet 4.0.0.0 252.0.0.0
object network 8.0.0.0-254.0.0.0
subnet 8.0.0.0 254.0.0.0
object network 11.0.0.0-255.0.0.0
subnet 11.0.0.0 255.0.0.0
object network 12.0.0.0-252.0.0.0
subnet 12.0.0.0 252.0.0.0
object network 16.0.0.0-240.0.0.0
subnet 16.0.0.0 240.0.0.0
object network 32.0.0.0-224.0.0.0
subnet 32.0.0.0 224.0.0.0
object network 64.0.0.0-224.0.0.0
subnet 64.0.0.0 224.0.0.0
object network 96.0.0.0-240.0.0.0
subnet 96.0.0.0 240.0.0.0
object network 112.0.0.0-248.0.0.0
subnet 112.0.0.0 248.0.0.0
object network 120.0.0.0-252.0.0.0
```



```
subnet 120.0.0.0 252.0.0.0
object network 124.0.0.0-254.0.0.0
subnet 124.0.0.0 254.0.0.0
object network 126.0.0.0-255.0.0.0
subnet 126.0.0.0 255.0.0.0
object network 128.0.0.0-224.0.0.0
subnet 128.0.0.0 224.0.0.0
object network 160.0.0.0-248.0.0.0
subnet 160.0.0.0 248.0.0.0
object network 168.0.0.0-255.0.0.0
subnet 168.0.0.0 255.0.0.0
object network 169.0.0.0-255.128.0.0
subnet 169.0.0.0 255.128.0.0
object network 169.128.0.0-255.192.0.0
subnet 169.128.0.0 255.192.0.0
object network 169.192.0.0-255.224.0.0
subnet 169.192.0.0 255.224.0.0
object network 169.224.0.0-255.240.0.0
subnet 169.224.0.0 255.240.0.0
object network 169.240.0.0-255.248.0.0
subnet 169.240.0.0 255.248.0.0
object network 169.248.0.0-255.252.0.0
subnet 169.248.0.0 255.252.0.0
object network 169.252.0.0-255.254.0.0
subnet 169.252.0.0 255.254.0.0
object network 169.255.0.0-255.255.0.0
subnet 169.255.0.0 255.255.0.0
object network 170.0.0.0-254.0.0.0
subnet 170.0.0.0 254.0.0.0
object network 172.0.0.0-255.224.0.0
subnet 172.0.0.0 255.224.0.0
object network 172.32.0.0-255.224.0.0
subnet 172.32.0.0 255.224.0.0
object network 172.64.0.0-255.192.0.0
subnet 172.64.0.0 255.192.0.0
object network 172.128.0.0-255.128.0.0
subnet 172.128.0.0 255.128.0.0
object network 173.0.0.0-255.0.0.0
subnet 173.0.0.0 255.0.0.0
object network 174.0.0.0-254.0.0.0
subnet 174.0.0.0 254.0.0.0
object network 176.0.0.0-240.0.0.0
subnet 176.0.0.0 240.0.0.0
object network 192.0.1.0-255.255.255.0
subnet 192.0.1.0 255.255.255.0
object network 192.0.3.0-255.255.255.0
subnet 192.0.3.0 255.255.255.0
object network 192.0.4.0-255.255.252.0
subnet 192.0.4.0 255.255.252.0
object network 192.0.8.0-255.255.248.0
subnet 192.0.8.0 255.255.248.0
object network 192.0.16.0-255.255.240.0
```



```
subnet 192.0.16.0 255.255.240.0
object network 192.0.32.0-255.255.224.0
subnet 192.0.32.0 255.255.224.0
object network 192.0.64.0-255.255.192.0
subnet 192.0.64.0 255.255.192.0
object network 192.0.128.0-255.255.128.0
subnet 192.0.128.0 255.255.128.0
object network 192.1.0.0-255.255.0.0
subnet 192.1.0.0 255.255.0.0
object network 192.2.0.0-255.254.0.0
subnet 192.2.0.0 255.254.0.0
object network 192.4.0.0-255.252.0.0
subnet 192.4.0.0 255.252.0.0
object network 192.8.0.0-255.224.0.0
subnet 192.8.0.0 255.248.0.0
object network 192.16.0.0-255.240.0.0
subnet 192.16.0.0 255.240.0.0
object network 192.32.0.0-255.224.0.0
subnet 192.32.0.0 255.224.0.0
object network 192.64.0.0-255.240.0.0
subnet 192.64.0.0 255.240.0.0
object network 192.80.0.0-255.248.0.0
subnet 192.80.0.0 255.248.0.0
object network 192.88.0.0-255.255.192.0
subnet 192.88.0.0 255.255.192.0
object network 192.88.64.0-255.255.224.0
subnet 192.88.64.0 255.255.224.0
object network 192.88.96.0-255.255.254.0
subnet 192.88.96.0 255.255.254.0
object network 192.88.98.0-255.255.255.0
subnet 192.88.98.0 255.255.255.0
object network 192.88.100.0-255.255.252.0
subnet 192.88.100.0 255.255.252.0
object network 192.88.104.0-255.255.248.0
subnet 192.88.104.0 255.255.248.0
object network 192.88.112.0-255.255.240.0
subnet 192.88.112.0 255.255.240.0
object network 192.88.128.0-255.255.128.0
subnet 192.88.128.0 255.255.128.0
object network 192.89.0.0-255.255.0.0
subnet 192.89.0.0 255.255.0.0
object network 192.90.0.0-255.254.0.0
subnet 192.90.0.0 255.254.0.0
object network 192.92.0.0-255.252.0.0
subnet 192.92.0.0 255.252.0.0
object network 192.96.0.0-255.224.0.0
subnet 192.96.0.0 255.224.0.0
object network 192.128.0.0-255.224.0.0
subnet 192.128.0.0 255.224.0.0
object network 192.160.0.0-255.248.0.0
subnet 192.160.0.0 255.248.0.0
object network 192.169.0.0-255.255.0.0
```



```
subnet 192.169.0.0 255.255.0.0
object network 192.170.0.0-255.254.0.0
subnet 192.170.0.0 255.254.0.0
object network 192.172.0.0-255.252.0.0
subnet 192.172.0.0 255.252.0.0
object network 192.176.0.0-255.240.0.0
subnet 192.176.0.0 255.240.0.0
object network 192.192.0.0-255.192.0.0
subnet 192.192.0.0 255.192.0.0
object network 193.0.0.0-255.0.0.0
subnet 193.0.0.0 255.0.0.0
object network 194.0.0.0-254.0.0.0
subnet 194.0.0.0 254.0.0.0
object network 196.0.0.0-252.0.0.0
subnet 196.0.0.0 252.0.0.0
object network 198.0.0.0-255.240.0.0
subnet 198.0.0.0 255.240.0.0
object network 198.16.0.0-255.254.0.0
subnet 198.16.0.0 255.254.0.0
object network 198.20.0.0-255.252.0.0
subnet 198.20.0.0 255.252.0.0
object network 198.24.0.0-255.248.0.0
subnet 198.24.0.0 255.248.0.0
object network 198.32.0.0-255.240.0.0
subnet 198.32.0.0 255.240.0.0
object network 198.48.0.0-255.254.0.0
subnet 198.48.0.0 255.254.0.0
object network 198.50.0.0-255.255.0.0
subnet 198.50.0.0 255.255.0.0
object network 198.51.0.0-255.255.192.0.0
subnet 198.51.0.0 255.255.192.0
object network 198.51.64.0-255.255.224.0
subnet 198.51.64.0 255.255.224.0
object network 198.51.96.0-255.255.252.0
subnet 198.51.96.0 255.255.252.0
object network 198.51.101.0-255.255.255.0
subnet 198.51.101.0 255.255.255.0
object network 198.51.102.0-255.255.254.0
subnet 198.51.102.0 255.255.254.0
object network 198.51.104.0-255.255.248.0
subnet 198.51.104.0 255.255.248.0
object network 198.51.112.0-255.255.240.0
subnet 198.51.112.0 255.255.240.0
object network 198.51.128.0-255.255.254.0
subnet 198.51.128.0 255.255.254.0
object network 198.52.0.0-255.252.0.0
subnet 198.52.0.0 255.252.0.0
object network 198.56.0.0-255.248.0.0
subnet 198.56.0.0 255.248.0.0
object network 198.64.0.0-255.192.0.0
subnet 198.64.0.0 255.192.0.0
object network 198.128.0.0-255.128.0.0
```



```
subnet 198.128.0.0 255.128.0.0
object network 199.0.0.0-255.0.0.0
subnet 199.0.0.0 255.0.0.0
object network 200.0.0.0-248.0.0.0
subnet 200.0.0.0 248.0.0.0
object network 208.0.0.0-240.0.0.0
subnet 208.0.0.0 240.0.0.0
```

```
object-group network TheInternet
network-object object 1.0.0.0-255.0.0.0
network-object object 2.0.0.0-254.0.0.0
network-object object 4.0.0.0-252.0.0.0
network-object object 8.0.0.0-254.0.0.0
network-object object 11.0.0.0-255.0.0.0
network-object object 12.0.0.0-252.0.0.0
network-object object 16.0.0.0-240.0.0.0
network-object object 32.0.0.0-224.0.0.0
network-object object 64.0.0.0-224.0.0.0
network-object object 96.0.0.0-240.0.0.0
network-object object 112.0.0.0-248.0.0.0
network-object object 120.0.0.0-252.0.0.0
network-object object 124.0.0.0-254.0.0.0
network-object object 126.0.0.0-255.0.0.0
network-object object 128.0.0.0-224.0.0.0
network-object object 160.0.0.0-248.0.0.0
network-object object 168.0.0.0-255.0.0.0
network-object object 169.0.0.0-255.128.0.0
network-object object 169.128.0.0-255.192.0.0
network-object object 169.192.0.0-255.224.0.0
network-object object 169.224.0.0-255.240.0.0
network-object object 169.240.0.0-255.248.0.0
network-object object 169.248.0.0-255.252.0.0
network-object object 169.252.0.0-255.254.0.0
network-object object 169.255.0.0-255.255.0.0
network-object object 170.0.0.0-254.0.0.0
network-object object 172.0.0.0-255.224.0.0
network-object object 172.32.0.0-255.224.0.0
network-object object 172.64.0.0-255.192.0.0
network-object object 172.128.0.0-255.128.0.0
network-object object 173.0.0.0-255.0.0.0
network-object object 174.0.0.0-254.0.0.0
network-object object 176.0.0.0-240.0.0.0
network-object object 192.0.1.0-255.255.255.0
network-object object 192.0.3.0-255.255.255.0
network-object object 192.0.4.0-255.255.252.0
network-object object 192.0.8.0-255.255.248.0
network-object object 192.0.16.0-255.255.240.0
network-object object 192.0.32.0-255.255.224.0
network-object object 192.0.64.0-255.255.192.0
network-object object 192.0.128.0-255.255.128.0
network-object object 192.1.0.0-255.255.0.0
network-object object 192.2.0.0-255.254.0.0
```



```
network-object object 192.4.0.0-255.252.0.0
network-object object 192.8.0.0-255.248.0.0
network-object object 192.16.0.0-255.240.0.0
network-object object 192.32.0.0-255.224.0.0
network-object object 192.64.0.0-255.240.0.0
network-object object 192.80.0.0-255.248.0.0
network-object object 192.88.0.0-255.255.192.0
network-object object 192.88.64.0-255.255.224.0
network-object object 192.88.96.0-255.255.254.0
network-object object 192.88.98.0-255.255.255.0
network-object object 192.88.100.0-255.255.252.0
network-object object 192.88.104.0-255.255.248.0
network-object object 192.88.112.0-255.255.240.0
network-object object 192.88.128.0-255.255.128.0
network-object object 192.89.0.0-255.255.0.0
network-object object 192.90.0.0-255.254.0.0
network-object object 192.92.0.0-255.252.0.0
network-object object 192.96.0.0-255.224.0.0
network-object object 192.128.0.0-255.224.0.0
network-object object 192.160.0.0-255.248.0.0
network-object object 192.169.0.0-255.255.0.0
network-object object 192.170.0.0-255.254.0.0
network-object object 192.172.0.0-255.252.0.0
network-object object 192.176.0.0-255.240.0.0
network-object object 192.192.0.0-255.192.0.0
network-object object 193.0.0.0-255.0.0.0
network-object object 194.0.0.0-254.0.0.0
network-object object 196.0.0.0-252.0.0.0
network-object object 198.0.0.0-255.240.0.0
network-object object 198.16.0.0-255.254.0.0
network-object object 198.20.0.0-255.252.0.0
network-object object 198.24.0.0-255.248.0.0
network-object object 198.32.0.0-255.240.0.0
network-object object 198.48.0.0-255.254.0.0
network-object object 198.50.0.0-255.255.0.0
network-object object 198.51.0.0-255.255.192.0.0
network-object object 198.51.64.0-255.255.224.0
network-object object 198.51.96.0-255.255.252.0
network-object object 198.51.101.0-255.255.255.0
network-object object 198.51.102.0-255.255.254.0
network-object object 198.51.104.0-255.255.248.0
network-object object 198.51.112.0-255.255.240.0
network-object object 198.51.128.0-255.255.254.0
network-object object 198.52.0.0-255.252.0.0
network-object object 198.56.0.0-255.248.0.0
network-object object 198.64.0.0-255.192.0.0
network-object object 198.128.0.0-255.128.0.0
network-object object 199.0.0.0-255.0.0.0
network-object object 200.0.0.0-248.0.0.0
network-object object 208.0.0.0-240.0.0.0
#####
```

## Cisco PIX “TheInternet” Object

```
#####  
#####  
# Cisco PIX group 'TheInternet' is made up of a list of IPv4 network  
# objects that are members of group 'TheInternet'  
# List is based upon RFC-5735 see http://tools.ietf.org/html/rfc5735  
# You should not be using PIX firewalls but if you are...  
#####  
#####  
# Check all of the information for errors and omissions.  
#####  
object-group network TheInternet  
network-object 1.0.0.0 255.0.0.0  
network-object 2.0.0.0 254.0.0.0  
network-object 4.0.0.0 252.0.0.0  
network-object 8.0.0.0 254.0.0.0  
network-object 11.0.0.0 255.0.0.0  
network-object 12.0.0.0 252.0.0.0  
network-object 16.0.0.0 240.0.0.0  
network-object 32.0.0.0 224.0.0.0  
network-object 64.0.0.0 224.0.0.0  
network-object 96.0.0.0 240.0.0.0  
network-object 112.0.0.0 248.0.0.0  
network-object 120.0.0.0 252.0.0.0  
network-object 124.0.0.0 254.0.0.0  
network-object 126.0.0.0 255.0.0.0  
network-object 128.0.0.0 224.0.0.0  
network-object 160.0.0.0 248.0.0.0  
network-object 168.0.0.0 255.0.0.0  
network-object 169.0.0.0 255.128.0.0  
network-object 169.128.0.0 255.192.0.0  
network-object 169.192.0.0 255.224.0.0  
network-object 169.224.0.0 255.240.0.0  
network-object 169.240.0.0 255.248.0.0  
network-object 169.248.0.0 255.252.0.0  
network-object 169.252.0.0 255.254.0.0  
network-object 169.255.0.0 255.255.0.0  
network-object 170.0.0.0 254.0.0.0  
network-object 172.0.0.0 255.224.0.0  
network-object 172.32.0.0 255.224.0.0  
network-object 172.64.0.0 255.192.0.0  
network-object 172.128.0.0 255.128.0.0  
network-object 173.0.0.0 255.0.0.0  
network-object 174.0.0.0 254.0.0.0  
network-object 176.0.0.0 240.0.0.0  
network-object 192.0.1.0 255.255.255.0  
network-object 192.0.3.0 255.255.255.0  
network-object 192.0.4.0 255.255.252.0  
network-object 192.0.8.0 255.255.248.0
```



network-object 192.0.16.0 255.255.240.0  
network-object 192.0.32.0 255.255.224.0  
network-object 192.0.64.0 255.255.192.0  
network-object 192.0.128.0 255.255.128.0  
network-object 192.1.0.0 255.255.0.0  
network-object 192.2.0.0 255.254.0.0  
network-object 192.4.0.0 255.252.0.0  
network-object 192.8.0.0 255.248.0.0  
network-object 192.16.0.0 255.240.0.0  
network-object 192.32.0.0 255.224.0.0  
network-object 192.64.0.0 255.240.0.0  
network-object 192.80.0.0 255.248.0.0  
network-object 192.88.0.0 255.255.192.0  
network-object 192.88.64.0 255.255.224.0  
network-object 192.88.96.0 255.255.254.0  
network-object 192.88.98.0 255.255.255.0  
network-object 192.88.100.0 255.255.252.0  
network-object 192.88.104.0 255.255.248.0  
network-object 192.88.112.0 255.255.240.0  
network-object 192.88.128.0 255.255.128.0  
network-object 192.89.0.0 255.255.0.0  
network-object 192.90.0.0 255.254.0.0  
network-object 192.92.0.0 255.252.0.0  
network-object 192.96.0.0 255.224.0.0  
network-object 192.128.0.0 255.224.0.0  
network-object 192.160.0.0 255.248.0.0  
network-object 192.169.0.0 255.255.0.0  
network-object 192.170.0.0 255.254.0.0  
network-object 192.172.0.0 255.252.0.0  
network-object 192.176.0.0 255.240.0.0  
network-object 192.192.0.0 255.192.0.0  
network-object 193.0.0.0 255.0.0.0  
network-object 194.0.0.0 254.0.0.0  
network-object 196.0.0.0 252.0.0.0  
network-object 198.0.0.0 255.240.0.0  
network-object 198.16.0.0 255.254.0.0  
network-object 198.20.0.0 255.252.0.0  
network-object 198.24.0.0 255.248.0.0  
network-object 198.32.0.0 255.240.0.0  
network-object 198.48.0.0 255.254.0.0  
network-object 198.50.0.0 255.255.0.0  
network-object 198.51.0.0 255.255.192.0  
network-object 198.51.64.0 255.255.224.0  
network-object 198.51.96.0 255.255.252.0  
network-object 198.51.101.0 255.255.255.0  
network-object 198.51.102.0 255.255.254.0  
network-object 198.51.104.0 255.255.248.0  
network-object 198.51.112.0 255.255.240.0  
network-object 198.51.128.0 255.255.254.0  
network-object 198.52.0.0 255.252.0.0  
network-object 198.56.0.0 255.248.0.0  
network-object 198.64.0.0 255.192.0.0





```
network-object 198.128.0.0 255.128.0.0  
network-object 199.0.0.0 255.0.0.0  
network-object 200.0.0.0 248.0.0.0  
network-object 208.0.0.0 240.0.0.0
```

#####

For additional information, contact [inquiry@wanegrity.com](mailto:inquiry@wanegrity.com)

<END>