pfSense - Feature #1901

Maintain IP range tables for popular Internet sites

09/25/2011 03:17 AM - Dim Hatz

Status:	Needs Patch	**Start date:**	09/25/2011
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Plus Target Version:		**Release Notes:**	Default

Description

Current version of pfsense includes the filterdns daemon which periodically resolves any fqdn in aliases into IP. But this won't work for Websites that return a different set of IPs on each DNS request, so the current solution seems to be doing URL filtering via a proxy like Squid+squidhuard. However this is of little help when a company has moved their email to Google and needs to access its servers via IMAP and wants to whitelist all Google's IPs. This scenario will come up more often, as companies migrate into SaaS and the cloud.

A solution would be for **pfsense to automatically keep track of certain sites' IP ranges** (e.g. GoogleApps). This info can be obtained via **whois** or **DNS**.

E.g. Google's ASN is 15169 https://www.dan.me.uk/bgplookup?asn=15169 or via DNS lookup of the SPF record, as Google suggests in "Google IP address ranges" page http://www.google.com/support/a/bin/answer.py?answer=60764

```
$ host -t txt _spf.google.com
_spf.google.com descriptive text "v=spf1 ip4:216.239.32.0/19 ip4:64.233.160.0/19 ip4:66.249.80.0/20 ip4:72.14.192.0/18
ip4:209.85.128.0/17 ip4:66.102.0.0/20 ip4:74.125.0.0/16 ip4:64.18.0.0/20 ip4:207.126.144.0/20 ip4:173.194.0.0/16 ?all"
```

History

#1 - 09/25/2011 03:35 AM - Dim Hatz

A somewhat related recent discussion http://forum.pfsense.org/index.php/topic,38741.0.html

#2 - 09/25/2011 03:43 AM - Seth Mos

For this to be useful or "complete" it would need a hybrid approach. You can't be sure that the spf record will also give you access to the google search and apps platforms.

I frequently run into this as well.

The idea of allowing a ASN number for firewall rules is tempting though, the easiest way to access this in a reasonably light fashion is by consulting a route-server that can give you all the networks.

This includes v6 and would make it worthwile. Pretty sure that route-servers have policies forbidding you to use it. I'd look into a package to see if that can work.

.. more thoughts. We could dump the ASN numbers to plain txt files to be picked up off a pfsense server or mirror. This could be done on a daily or hourly basis, as long as we have access to a route-server.
Another thought that just occured is that this would work really well for google, but not quite so well for other non content networks. Granular it isn't

#3 - 09/25/2011 07:42 PM - Dim Hatz

"We could dump the ASN numbers to plain txt files to be picked up off a pfsense server or mirror"

Right, that would be another viable option, much like the /etc/rc.update_bogons.sh does for bogons.

Actually there are a number of txt files containing IP ranges in CIDR notation that could be added to pfSense (and I've seen them being used in other software firewalls) with scripts very much like the rc.update_bogons.sh-script, e.g. the lists by dshield.org or spamhaus.org e.g.

http://www.spamhaus.org/drop/drop.lasso
DROP (Don't Route Or Peer) is an advisory "drop all traffic" list, consisting of stolen 'hijacked' netblocks and netblocks controlled entirely by professional spammers. DROP is a tiny subset of the SBL designed for use by firewalls and routing equipment.

DShield's current Most Active Attacking IPs
http://feeds.dshield.org/top10-2.txt
(Same data as is used on DShield.org Top 10 Most Wanted.)
0 = IP Address, 1 = Resolved domain of IP Address

etc

And such a targeted approach is much better than blocking entire countries, as some people do.

#4 - 09/25/2011 08:02 PM - Jim Pingle

Lists like that can be added as URL table aliases in 2.0 (though the code may need adjusting so it only grabs the first parameter of the line in those format files). URL Table Aliases are aliases pointed at an arbitrary URL that contains a text list of CIDR networks, then you can use that alias in firewall rules however you like. The list is updated periodically.

#5 - 10/10/2011 10:00 AM - Ermal Luçi

The only option here is to create a transparent proxy for dns and hook that up with daemons as filterdns.
All other options will have their drawbacks.

#6 - 10/10/2011 12:04 PM - Dim Hatz

Sure if you would want to "cover all the bases" you'd need to monitor DNS traffic and add IPs to the passthrough list, however for starters it could be something much simpler, like an enhanced version of /etc/rc.update_urltables with the changes that jimp mentioned (BTW note that the "Update Freq." option is inactive in firewall_aliases_edit.php in 2.0REL).

#7 - 10/15/2011 07:56 AM - Ermal Luçi

I do not like that since you cannot draw the line what is more important and what is to skip.

#8 - 09/04/2013 11:04 AM - Chris Buechler

- Status changed from New to Needs Patch