pfSense - Feature #3199

Option to accumulate or not IP addresses in Alias table of FQDNs

09/14/2013 11:30 PM - Phillip Davis

Status:	Resolved	**Start date:**	09/14/2013
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Rules / NAT	**Estimated time:**	0.00 hour
Target version:	2.2.1		
Plus Target Version:		**Release Notes:**	Default

Description

As at the time of writing, an Alias of FQDNs gets the FQDNs translated to the corresponding IP addresses and a table is created in pf containing these addresses. The FQDN translations are checked every so often (5 minutes by default) and if the FQDN now translates to a different IP address, that new IP address is added to the table. So the table gradually gets bigger.
Sometimes this behaviour is desired - e.g. FQDNs like "facebook.com", "google.com", "yahoo.com" that are a "revolving door" of IP addresses. The admin might want the system to gradually accumulate the known IP addresses for the FQDN/s and have some firewall rule/s apply to pass or block the whole set of known addresses. (admittedly this is not very effective!)
But sometimes this behaviour is not required. For example, a list of the FQDNs that translate to dynamic IPs of remote offices which make site-to-site connections into a central office. The remote office updates its dynamic DNS when its public IP address changes. 5 minutes later, the alias at the server end is checked and updated. There is a firewall rule allowing only connections into the site-to-site OpenVPN server from the FQDNs in the alias. In this case the table for the alias should ONLY have the current IP address corresponding to each FQDN.
Proposed solution: have an attribute of an alias that is a checkbox (boolean) so the admin can decide to select "accumulate all known IP addresses for this alias", or not (meaning keep only the latest IP address for each FQDN in the table).

History

#1 - 09/14/2013 11:33 PM - Phillip Davis

A bit of relevant discussion at http://forum.pfsense.org/index.php/topic,66300.0.html

#2 - 12/13/2013 12:54 AM - Steve Reinhardt

I just ran into this problem, and I'd consider it a bug that needs to be fixed, not a feature request. I was using an alias to contain a list of hosts (given as FQDNs) to block (coincidentally, exactly the example given at https://doc.pfsense.org/index.php/Aliases). I needed to unblock a host, so I removed it from the alias, and clicked the button to update the rules. I thought I might have to wait a while for the update to take effect, but a half hour later, it was pretty clear that it wasn't going to happen. So I started poking around and found that 'pfctl -T show -t Blocked' still had all the original IPs in it, even though /var/etc/filterdns.conf had been updated.

Clearly I'm running into the same "feature" described above, but from my perspective it sure seems like plain old brokenness. I didn't want to file a separate bug report right away though, since the issue is already recorded here.

#3 - 12/13/2013 02:28 AM - Phillip Davis

I just double-checked this now that 2.1-RELEASE has been out an running for ages. I have a table of the IPs of all my organisation offices, which are dynamic and the ISPs concerned seem to reset things regularly, so the dynamic public IPs change often. There will be 15 real current public IPs, so I would like the table to have 15 entries, but the table has now accumulated 1084 IP address entries on a router that has been up for 30 days. So 2.1-RELEASE is definitely accumulating addresses into the table and not removing old ones.
I'm not sure that this behaviour is strictly a bug, since there is no requirement or design spec that I know of that defines what it is required to do :)

#4 - 12/14/2013 01:29 AM - Steve Reinhardt

Thanks for the confirmation. Sorry, forgot to mention that I'm running 2.1-RELEASE as well.

It seems like a bug to me because, (1) even if the spec doesn't specifically say that removing an FQDN from the alias in the GUI also removes it from the corresponding pf table, the fact that it doesn't is totally counterintuitive that you'd think it would be documented if it were intended, and (2) if you use IPs rather than FQDNs, removing an entry from an alias does remove it from the table (afaict), and other than the five-minute delay for running through DNS, there's no documentation or reasonable expectation that aliases would have such radically different behavior depending on whether you use IPs or FQDNs.

#5 - 12/22/2013 12:20 PM - Ermal Luçi

Normally this will be fixed when filterdns supports reloading with TTL of the DNS record.
This will come soon.

#6 - 02/06/2014 09:36 AM - Kurian Thampy

I don't see any reason to accumulate addresses at all. DNS A records for an FQDN return all valid addresses at once. It's up to the client to choose which one, usually choosing the first one. The server only mixes up the order each time thus creating a round robin effect since the client almost always uses the first address.

Basically you should wipe out all existing addresses each time you requery.

#7 - 02/09/2015 11:22 PM - Chris Buechler

- Status changed from New to Resolved

- Target version changed from Future to 2.2.1

this was done in 2.2-RELEASE (can't set that as target since it's closed).

Files

RemoteOffices.png	25.8 KB	09/15/2013	Phillip Davis