pfSense - Bug #5806

Alias URL table containing an unresolvable FQDN entry causes rules to not load

01/23/2016 03:02 PM - robi robi

Status:	Closed	**Start date:**	01/23/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Aliases / Tables	**Estimated time:**	0.00 hour
Target version:			
Plus Target Version:		**Affected Version:**	All
Release Notes:		**Affected Architecture:**	

Description

Set up an URL alias pointing to an internal http resource, listing about 25 entries, each a public FQDN.
Set up a port forward on the WAN interfaces, specifying as source the URL alias.
If for some reason one of the FQDN entries in the list becomes unresolvable (for example pinging it from command line gives back "ping: cannot resolve example.com: unknown host"), the whole firewall breaks.
No more NAT through pfSense (I can ping google.com from pfSense box, but cannot ping it from any network behind it). There are alerts in the web interface complaining that the file containing the list in /var/db/aliastables/ is invalid, these get also registered in the system log.
Routing without NAT seems to work between local interfaces, but I couldn't access remote sites through VPN, which are NATted on their virtual interfaces.

This happens on a C2758 system, with amd64 architecture NanoBSD.

Temporary solution (outside pfSense) was to add FQDN > IP translation and validation on the internal server (using php gethostbyname() and ip2long()), so that the URL alias always gets existing IP addresses and not FQDNs, which may be unresolvable.

A fix on pfSense would be when an URL alias contains names, skip the ones not resolving, and not try to add to the table.

History

#1 - 01/23/2016 03:09 PM - robi robi

Happened on v2.2.6, and reproduced on v2.2.4 too, but with a different error in the system log.
Removing the problematic FQDN address from the list doesn't fix it, the table gets created, but traffic still doesn't get through.

The only remedy is to reboot.

Unfortunately can't quote the exact errors from the log, because they are not saved on NanoBSD.

#2 - 01/26/2016 04:28 PM - Chris Buechler

- Category set to Operating System

- Status changed from New to Confirmed

- Priority changed from High to Normal

- Affected Version set to All

You end up with a syntax error that prevents loading of the ruleset in that case.

```
no IP address found for google.com
/tmp/rules.debug:29: file "/var/db/aliastables/test.txt" contains bad data
```

Putting the FQDNs directly into a host alias won't do that since filterdns handles the name resolution and table manipulation then.

#3 - 01/27/2016 03:32 AM - robi robi

Yes, that's exactly the error mesage I was seeing. Thank you.

#4 - 07/10/2016 12:25 AM - Chris Buechler

- Subject changed from Alias URL table containing an unresolvable FQDN entry breaks the whole firewall to Alias URL table containing an unresolvable FQDN entry causes rules to not load

- Category changed from Operating System to Rules / NAT

#5 - 08/21/2019 11:01 AM - Jim Pingle

- Category changed from Rules / NAT to Aliases / Tables

#6 - 03/26/2020 01:55 AM - Viktor Gurov

- Status changed from Confirmed to Closed

no such issue on 2.4.5 and 2.5.0.a.20200324.1145
it ignores unresolved hosts, putting only valid IPs in /var/db/aliastables/test.txt