

pfSense - Bug #15071

Applying interface changes may not update default ACLs for the DNS Resolver

12/06/2023 05:19 PM - George Phillips

Status:	Resolved	Start date:	
Priority:	Normal	Due date:	
Assignee:	Marcos M	% Done:	100%
Category:	DNS Resolver	Estimated time:	0.00 hour
Target version:	2.8.0	Affected Version:	
Plus Target Version:	24.03	Affected Architecture:	All
Release Notes:	Default		
Description			
To reproduce:			
1. Base install of pfSense Plus 23.09 with 1 LAN and 1 WAN			
2. Activate an OPT interface and give it an IP/mask (in our case, 172.17.2.1/24)			
3. cat /var/unbound/access_lists.conf			
4. Notice that the network 172.17.2.0/24 is not present.			
Attempted to restart unbound, but that did not fix it.			
Manually adding the network to access-list via GUI creates the entry in access_lists.conf			
After removing the access-list entry via GUI, the network entry remains in access_lists.conf			
Related issues:			
Has duplicate Bug #14631: ACL on DNS Resolver is not updated list after IPs c...			Duplicate

Associated revisions

Revision fbc8d7d0 - 12/08/2023 06:19 PM - Marcos M

Check "all" when restarting unbound based on interface. Fix #15071

History

#1 - 12/06/2023 05:22 PM - Steve Wheeler

- Target version set to 24.03
- Affected Architecture All added

Resaving the Unbound config in the gui correctly creates the ACL file with the new subnet.

It appears to not be triggered as expected by the addition of the new subnet.

#2 - 12/06/2023 05:38 PM - Jim Pingle

Steve Wheeler wrote in [#note-1](#):

Resaving the Unbound config in the gui correctly creates the ACL file with the new subnet.

It appears to not be triggered as expected by the addition of the new subnet.

IIRC that's been the case for a while. There were similar behaviors noted in other areas like OpenVPN ([#12991](#)). Though if it worked in the past, it's also possible interface behavior regressed more recently as a consequence of other changes (e.g. DHCP registration changes due to Kea integration).

#3 - 12/08/2023 06:24 PM - Marcos M

- Project changed from pfSense Plus to pfSense
- Subject changed from New interfaces are not added to default ACL in Unbound to Applying interface changes may not update unbound's default ACL

- Category changed from DNS Resolver to DNS Resolver
- Assignee set to Marcos M
- Target version changed from 24.03 to 2.8.0
- Affected Plus Version deleted (23.09)
- Plus Target Version set to 24.03

#4 - 12/08/2023 06:29 PM - Marcos M

- Status changed from New to Feedback

Fixed in fbc8d7d04dc5f7cbec65381b81dc5f4eed06a714.

#5 - 12/08/2023 06:29 PM - Marcos M

- % Done changed from 0 to 100

#6 - 12/09/2023 07:38 AM - Danilo Zrenjanin

- Status changed from Feedback to Resolved

Tested the patch on 23.09.

The patch fixes all reported misbehavior.

I am marking this ticket reslvoed.

#7 - 12/09/2023 07:41 AM - Lev Prokofev

- File clipboard-202312091440-orqyk.png added

Tested the patch on

23.09.1-RELEASE (arm64)
built on Wed Dec 6 23:22:00 MSK 2023
FreeBSD 14.0-CURRENT

Saving the Interface now triggers the ACL to rewrite,

```
[23.09.1-RELEASE] [root@pfSense.georgia.arpa]/root: cat  
.conf  
access-control: 127.0.0.1/32 allow_snoop  
access-control: ::1 allow_snoop  
access-control: 10.6.210.0/31 allow  
access-control: 127.0.0.0/8 allow  
access-control: 172.17.2.0/24 allow  
access-control: 172.21.100.0/24 allow  
access-control: 192.168.41.0/24 allow  
access-control: ::1/128 allow  
[23.09.1-RELEASE] [root@pfSense.georgia.arpa]/root: 
```

#8 - 12/20/2023 05:58 PM - Marcos M

- Has duplicate Bug #14631: ACL on DNS Resolver is not updated list after IPs changed on interfaces added

#9 - 02/05/2024 08:18 PM - Jim Pingle

- Subject changed from Applying interface changes may not update unbound's default ACL to Applying interface changes may not update default ACLs for the DNS Resolver

Files

Screenshot 2023-12-06 at 12.09.13 PM.png	133 KB	12/06/2023	George Phillips
clipboard-202312091440-orqyk.png	15 KB	12/09/2023	Lev Prokofev