## pfSense - Regression #11805

## Port forward rules only function through the default gateway interface, ``reply-to`` does not work for Multi-WAN (CE Only)

04/14/2021 07:35 AM - Jim Pingle

| | | | |
|---|---|---|---|
| **Status:** | Resolved | **Start date:** | 04/14/2021 |
| **Priority:** | Urgent | **Due date:** | |
| **Assignee:** | Kristof Provost | **% Done:** | 0% |
| **Category:** | Rules / NAT | **Estimated time:** | 0.00 hour |
| **Target version:** | 2.5.2 | | |
| **Plus Target Version:** | | **Affected Version:** | 2.5.1 |
| **Release Notes:** | Default | **Affected Architecture:** | amd64 |

### Description

Port forwards coming into the firewall from a non-default WAN are not working properly on CE version 2.5.1. This is similar to #11436 but now happening on CE only, not Plus 21.02.2.

Unlike before, there is no firewall log entry for the packet attempting to leave via the wrong path.

Packet capture on WAN2 shows the SYN arriving, but no response.

State table shows:

```
vmx3 tcp 127.0.0.1:22 (203.0.113.3:222) <- 172.21.32.79:60472       CLOSED:SYN_SENT
   [0 + 64240]  [2247652855 + 1]
   age 00:00:04, expires in 00:00:29, 3:5 pkts, 180:300 bytes, rule 158
   id: 0100000060774d99 creatorid: e2ca2a66
```

Rule 158 created the state, and it is:

```
@158(1617127544) pass in quick on vmx3 reply-to (vmx3 203.0.113.1) inet proto tcp from any to 127.
0.0.1 port = ssh flags S/SA keep state label "USER_RULE: NAT Reply-to test WAN2"
  [ Evaluations: 23443     Packets: 59        Bytes: 3540        States: 0     ]
  [ Inserted: pid 72469 State Creations: 4     ]
```

Contacting a service directly on WAN2, not via port forwarding, works.

### History

#### #1 - 04/14/2021 08:16 AM - Kristof Provost

I can't seem to reproduce this on my system, running 'pfSense 2.5.1-RELEASE (amd64) on pfSense'. Can you share your rules file (and perhaps the configuration file)?

#### #2 - 04/14/2021 08:37 AM - Kristof Provost

Correction, I was testing it wrong, I can reproduce. I'd again forgotten to ensure my requests came from outside the WAN/WAN2 subnets.

#### #3 - 04/14/2021 03:32 PM - Kristof Provost

I'm confident I have a fix ready. It's being reviewed & validated internally.

**#4 - 04/15/2021 11:56 AM - Kristof Provost**

Patrick Clara: I cannot tell from that post if this is the same problem or not. It could plausibly be.

2.6.0 working matches what I'd expect from what I know the issue to be.

**#5 - 04/15/2021 11:59 AM - Rajil Saraswat**

@Kristof, will there be a point release to fix this, or can a patch be applied to 2.5.1?

I guess a point release would take some time to roll out.

**#6 - 04/17/2021 09:18 AM - Jim Pingle**

We have more than enough confirmation that it's a problem at this point, please refrain from commenting to that effect. I'll be cleaning up some of the older comments here that aren't adding anything substantial to the development process, since it makes finding relevant information on the issue difficult.

EDIT: 25 comments removed.

**#7 - 04/17/2021 12:00 PM - Luca De Andreis**

I would just like to add that on a multi gateway firewall (typically, in my case, wan and mpls) there is a loss of the connection after 30 seconds if the connection request occurs not through the default gateway (for example if I reach an internal network segment to the firewall with a connection coming from the mpls gateway if the default gateway is wan). Loss of connection after 30 seconds (approximately) results in a reconnection of rdp or a freeze of ssh. Of course the same configuration works perfectly with the 245p1 version.

**#8 - 04/20/2021 06:41 PM - Reinaldo Alves Feitosa**

I also have the same problem!

**#9 - 04/21/2021 01:05 AM - Kristof Provost**

Adam Kuklycz wrote:

> Now, with Jim removing a handful of comments saying they too have the issue, it gives the perception that this issue is a lot less and maybe not even related to the problem others are having, so while it does clean up the issue it makes the end user less certain that it affects them or not. It also makes me feel uncomfortable, thinking that this problem may not get addressed anytime in the near future. The issue hasn't been assigned a priority...nothing...

Jim removed those because "Me too!" does not contribute anything to the bug report, but obscures relevant information.
The fix has been committed and will be included in the next release. I do not know when that will be.

**#10 - 04/21/2021 07:16 AM - Jim Pingle**

*- Status changed from New to Feedback*

*- Priority changed from Normal to Urgent*

*- Target version changed from CE-Next to 2.6.0*

I cleaned up the comments again. **Please do not comment unless you have substantial new information**. Otherwise, keep the discussion on the forum. We are well aware of the impact the issue has, and if you look at my previous comment I've noted how many comments were removed. Thus keeping a lot of "me too" posts here only serves to obscure meaningful development discussion.

This is not a configuration or PHP code issue, but an issue in the kernel, so it is not possible to patch it in-place and an upgrade is required. If you want to test it, try a 2.6.0 snapshot.

#### #11 - 04/21/2021 09:42 AM - Emanuel Birkmann

I don't know if this is substantial new information, especially if a fix is already under development. But what I figured out and what seems to be nowhere reported so far - as far as I can tell - is the fact that in a packet capture I could see the outgoing responses to packets coming in on the non-default WAN interface but they were tried to be sent to the internet with the private RFC1918 IP address of the responding server. So, incoming, the port forwarding is working as expected, the server answers correctly, but outgoing, NAT is not applied. But at least, the responses went out on the correct non-default WAN interface. My first assumption was that the responses might be going out on the default WAN interface instead.

#### #12 - 04/21/2021 09:48 AM - Jim Pingle

2.6.0 snapshots are currently working correctly, and the fix was checked into RELENG_2_5_0. Whatever release happens next will behave correctly either way (e.g. a 2.6.0 release or a 2.5.x point or patch release).

#### #13 - 04/27/2021 08:53 AM - Jens Groh

Jim Pingle wrote:

> 2.6.0 snapshots are currently working correctly, and the fix was checked into RELENG_2_5_0. Whatever release happens next will behave correctly either way (e.g. a 2.6.0 release or a 2.5.x point or patch release).

If you don't mind: if the fix was checked into RELENG_2_5_0, could you post the fix/patch ID so one could cherry pick it via system patches and test it? There are many users and clients waiting for their multiWAN to run cleanly again and feedback/helping catch flaws would surely be better if more could already test the proposed fix!

Thanks,
Jens

#### #14 - 04/27/2021 08:56 AM - Jim Pingle

Jens Groh wrote:

> If you don't mind: if the fix was checked into RELENG_2_5_0, could you post the fix/patch ID so one could cherry pick it via system patches and test it? There are many users and clients waiting for their multiWAN to run cleanly again and feedback/helping catch flaws would surely be better if more could already test the proposed fix!

It is a kernel-level fix, not something that can be applied as a patch using that package.

**#15 - 05/01/2021 05:19 PM - Rafael Possamai**

> It is a kernel-level fix, not something that can be applied as a patch using that package.

Jim, thanks for the updates. Do you have a link for the upstream bug report, or was this introduced by a Netgate patch? Thanks.

**#16 - 05/11/2021 03:43 PM - Jim Pingle**

*- Plus Target Version set to 21.05*

**#17 - 05/11/2021 03:52 PM - Jim Pingle**

*- Plus Target Version deleted (21.05)*

Actually this was fixed in the previous Plus release so not relevant to Plus. Taking back off.

**#18 - 05/24/2021 08:55 AM - Tom Davis**

Hi, just want to report its working fine now for me using the latest dev CE version 2.6.0.a.20210524.0100
More details: Running in Hyper-V, Gateway group Load balancing with 3 Tier 1 Openvpn Gateways.
For me, 2.5.0-dev broke the Gateway Group. 2.5.1 broke Port forward and fixed Gateway Groups, 2.6.0.a fixed them both.
Regards,
Thanks for all the great work!
-TD

**#19 - 05/24/2021 09:02 AM - Vikash Jhagroe**

Tom Davis wrote:

> Hi, just want to report its working fine now for me using the latest dev CE version 2.6.0.a.20210524.0100
> More details: Running in Hyper-V, Gateway group Load balancing with 3 Tier 1 Openvpn Gateways.
> For me, 2.5.0-dev broke the Gateway Group. 2.5.1 broke Port forward and fixed Gateway Groups, 2.6.0.a fixed them both.
> Regards,
> Thanks for all the great work!
> -TD

Thnx for your feedback, we already know this bug is fixed in the upcoming 2.6. I hope you are seriously not running a DEVELOPMENT RELEASE in a production environment. Running a DEVELOPMENT release is not the fix for this bug in a PRODUCTION environment.

**#20 - 05/27/2021 08:02 AM - Jim Pingle**

*- Target version changed from 2.6.0 to 2.5.2*

**#21 - 06/01/2021 10:20 AM - Jim Pingle**

Testing on 2.5.2-BETA snapshot build 2.5.2.b.20210601.0300 confirms it is fixed there on a system which could reproduce the problem on 2.5.1.

Will hold open for now to wait for additional feedback, but can be closed if none is received before release.

**#22 - 06/03/2021 12:55 PM - Jim Pingle**

*- Subject changed from Port forward works only on interface with default gateway, does not work for alternative wans (CE Only) to Port forward rules only function through the default gateway interface, ``reply-to`` does not work for Multi-WAN (CE Only)*

Updating subject for release notes.

**#23 - 06/06/2021 11:10 PM - Adam Kuklycz**

Question, does this affect virtual IP's that are setup on the same interface as the default gateway IP, or does the IP address have to be on a physically different interface/wan for it to become an issue?

**#24 - 06/07/2021 07:41 AM - Jim Pingle**

Adam Kuklycz wrote:

> Question, does this affect virtual IP's that are setup on the same interface as the default gateway IP, or does the IP address have to be on a physically different interface/wan for it to become an issue?

As far as I'm aware it should not affect that scenario since the VIP is on the same interface as the default route. The problem scenario is when the return traffic must take a different path back to the original origin of the request. So long as the traffic comes in and out on the default route WAN that is OK.

**#25 - 06/09/2021 10:15 AM - Bouke Henstra**

Jim Pingle wrote:

> Adam Kuklycz wrote:
>
> > Question, does this affect virtual IP's that are setup on the same interface as the default gateway IP, or does the IP address have to be on a physically different interface/wan for it to become an issue?
>
> As far as I'm aware it should not affect that scenario since the VIP is on the same interface as the default route. The problem scenario is when the return traffic must take a different path back to the original origin of the request. So long as the traffic comes in and out on the default route WAN that is OK.

I did notice issues with a routed subnet via GRE. This traffic flows through the same WAN interface too. But that's technically something else than a virtual IP.

**#26 - 06/10/2021 07:36 AM - Renato Botelho**

*- Status changed from Feedback to Resolved*

Bouke Henstra wrote:

> Jim Pingle wrote:
>
> > Adam Kuklycz wrote:
> >
> > > Question, does this affect virtual IP's that are setup on the same interface as the default gateway IP, or does the IP address have to be on a physically different interface/wan for it to become an issue?
> >
> > As far as I'm aware it should not affect that scenario since the VIP is on the same interface as the default route. The problem scenario is when the return traffic must take a different path back to the original origin of the request. So long as the traffic comes in and out on the default route WAN that is OK.
>
> I did notice issues with a routed subnet via GRE. This traffic flows through the same WAN interface too. But that's technically something else than a virtual IP.

Please open a new bug with details about how to reproduce.

This specific issue is fixed.