pfSense Plus - Regression #11436

State matching problem with reponses to packets arriving on non-default WANs

02/17/2021 04:28 PM - Grzegorz Krzystek

Status:	Resolved	**Start date:**	02/17/2021
Priority:	Very High	**Due date:**	
Assignee:	Kristof Provost	**% Done:**	100%
Category:	Rules / NAT	**Estimated time:**	0.00 hour
Target version:	21.02.2		
Release Notes:	Default	**Affected Architecture:**	All
Affected Plus Version:			

Description

I have quite specific multiwan setup
WAN (symmetric pppoe) port forward for ssh to lan (rpi)
WAN2 (symmetric commercial link over vlan) a lot port forwards to DMZ_LAN

LAN have clasical failover to "prefer PPPOE link over WAN2"
DMZ_LAN have all outgoing traffic set to go via "WAN2_GATEWAY"

Default gateway for pfsense is set to "prefer PPPOE link over WAN2"

now the problem is that after update to 21.02 all port forwards on WAN2 interface stopped working.
only way to make them work is to switch pfsense default gateway to wan2 , but then portforwards stops working on WAN...

History

#1 - 02/18/2021 06:16 AM - DRago_Angel [InV@DER]

Have same issue, started on devel 2.5. Posted some details at
https://forum.netgate.com/topic/159354/pfsense-2-5-0-a-20201127-0650-nat-issues/15?_=1609081294703

#2 - 02/18/2021 02:45 PM - Jim Pingle

- Tracker changed from Bug to Regression

- Subject changed from 21.02 Port forward works only on interface with default gateway, does not work for alternative wans to Port forward works only on interface with default gateway, does not work for alternative wans

- Target version set to CE-Next

- Affected Version set to 2.5.0

I can reproduce this here as well. It was working not too long ago, though. It doesn't seem to affect everything, however, since my OpenVPN multi-home setup which uses port forwards to 127.0.0.1 still functions on both WANs.

Same port forward on WAN (igb2) and WAN2 (pppoe0). Rule is at the top and present on both interfaces. Client connects to WAN port forward fine, but not WAN2.

tcpdump on WAN2 shows the client sends a SYN in on pppoe0. The SYN exits LAN, the reply SYN+ACK comes back in LAN, but no packet leaves. I've captured on other interfaces (including the default WAN) and I don't see the reply exit the firewall.

Packet capture on WAN2:

```
15:31:45.647541 AF IPv4 (2), length 64: (tos 0x0, ttl 45, id 7098, offset 0, flags [DF], proto TCP (6), length
 60)
    cli.ent.cli.ent.6236 > wan.two.wan.two.58020: Flags [S], cksum 0xde30 (correct), seq 2689546114, win 65535
, options [mss 1388,sackOK,TS val 3402388902
ecr 0,nop,wscale 8], length 0
15:31:46.707231 AF IPv4 (2), length 64: (tos 0x0, ttl 45, id 7099, offset 0, flags [DF], proto TCP (6), length
 60)
    cli.ent.cli.ent.6236 > wan.two.wan.two.58020: Flags [S], cksum 0xda44 (correct), seq 2689546114, win 65535
```

```
, options [mss 1388,sackOK,TS val 3402389906
ecr 0,nop,wscale 8], length 0
15:31:48.666981 AF IPv4 (2), length 64: (tos 0x0, ttl 45, id 7100, offset 0, flags [DF], proto TCP (6), length
 60)
    cli.ent.cli.ent.6236 > wan.two.wan.two.58020: Flags [S], cksum 0xd276 (correct), seq 2689546114, win 65535
, options [mss 1388,sackOK,TS val 3402391904
ecr 0,nop,wscale 8], length 0
15:31:50.607698 AF IPv4 (2), length 64: (tos 0x0, ttl 45, id 26598, offset 0, flags [DF], proto TCP (6), lengt
h 60)
    cli.ent.cli.ent.6238 > wan.two.wan.two.58020: Flags [S], cksum 0xddc1 (correct), seq 218413056, win 65535,
 options [mss 1388,sackOK,TS val 3402393824 e
```

State table entry:

```
pppoe0 tcp iii.iii.iii.iii:8020 (wan.two.wan.two:58020) <- cli.ent.cli.ent:6238       SYN_SENT:ESTABLISHED
   [1582840280 + 65536] wscale 7  [218413056 + 65281] wscale 8
   age 00:00:09, expires in 00:00:28, 1:4 pkts, 60:240 bytes, rule 393
```

Relevant rule (which created the above state entry):

```
@393(1613679975) pass in quick on pppoe0 reply-to (pppoe0 gw.gw.gw.gw) inet proto tcp from any to iii.iii.iii.
iii port = 8020 flags S/SA keep state label
 "USER_RULE: NAT Test NAT to NUC"
  [ Evaluations: 895       Packets: 159       Bytes: 9540        States: 6     ]
  [ Inserted: pid 28039 State Creations: 18    ]
```

#3 - 03/03/2021 07:38 AM - Jim Pingle

- Has duplicate Bug #11611: Multi WAN Static Routes & NAT failure on multiple interfaces added

#4 - 03/05/2021 09:59 AM - Marcos Mendoza

Another report:

Port forward and firewall rules are in place on a secondary PPPoE WAN interface. Traffic comes in, gets NATed, then gets dropped when going outbound on PPPoE interface by the following rule:

```
block out log inet all tracker 1000000104 label "Default deny rule IPv4"
```

Adding a floating rule didn't help:

```
pass  out log  quick  on {  pppoe1  } reply-to ( pppoe1 x.x.x.x ) inet proto { tcp udp }  from any port 53 to
any tracker 1614956436 keep state  label "USER_RULE: TEST"
```

The traffic did not show as blocked on the logs anymore, but it also didn't succeed either given it was timing out. After creating the floating rule, there were some instances (not triggered by the test traffic) where the rule matched:

```
@195(1614956436) pass out log quick on pppoe1 reply-to (pppoe1 x.x.x.x) inet proto tcp from any port = domain
to any flags S/SA keep state label "USER_RULE: TEST"
  [ Evaluations: 13547     Packets: 0         Bytes: 0           States: 0     ]
  [ Inserted: pid 13655 State Creations: 0     ]
@196(1614956436) pass out log quick on pppoe1 reply-to (pppoe1 x.x.x.x) inet proto udp from any port = domain
to any keep state label "USER_RULE: TEST"
  [ Evaluations: 118       Packets: 2         Bytes: 260         States: 1     ]
  [ Inserted: pid 13655 State Creations: 2     ]
```

```
pppoe1 udp y.y.y.y:53 -> a.a.a.a:8730       SINGLE:NO_TRAFFIC
   age 00:00:31, expires in 00:00:29, 1:0 pkts, 130:0 bytes, rule 196
   id: 02000000605c4cce creatorid: babfe159
```

I noticed the PPPoE gateway that was automatically created was outside of the subnet of the interface IP and did not show the "enabled" checkmark under "System / Routing / Gateways". After editing it and checking "Use non-local gateway", the gateway showed as enabled. However, the tests results did not change.

#5 - 03/05/2021 10:23 AM - Grzegorz Krzystek

Marcos Mendoza wrote:
[...]

> I noticed the PPPoE gateway that was automatically created was outside of the subnet of the interface IP and did not show the "enabled" checkmark under "System / Routing / Gateways". After editing it and checking "Use non-local gateway", the gateway showed as enabled. However, the tests results did not change.

[...]

i have nonlocal gateway on pppope , and it works fine without checked nonlocal gateway. (can't reproduce that) in my case WAN_PPPOE have GW : 72.16.220.2 , wile ip is from 193.107.248.XXX net.
with PPP intrafaces such practice is normal. and it works even with allow nonlocal gateway disabled - tested it on clean config 10 minutes ago. so that's not a case, and reported tace need to be investigated deeper.

#6 - 03/07/2021 11:21 AM - Steve Wheeler

It looks like the reply traffic is not matching the state created by the inbound connection on the WAN.

The firewall logs shows it blocked outbound as flagged TCP traffic. Similar to the GRE/IPSec bug and we can deploy a similar workaround using a floating outbound rule with any tcp flags and sloppy states enabled.

However traffic still fails. It's no longer blocked but ACK packets are not forwarded after applying that.

#7 - 03/08/2021 09:17 AM - R M

Same issue here after upgrade to v21.02,
MultiWan wont NAT properly on both wan.
A new message to let you know this is affecting also openvpn client acces (but still working site to site)
Good luck on resolving it
Thank you

#8 - 03/08/2021 09:46 AM - Viktor Gurov

the last filter generating change is
https://github.com/pfsense/pfsense/commit/fce8a99bffae47c965c692dbe763ae9732092f95#diff-363a5fb2c2d253691939c4a41c5c0b2196dabdbd3d16d770c2a1300a46be577c

and it adds IP protocol definition, i.e.:
rdr on vtnet2 **inet** proto tcp from any to 172.16.16.41 port 2000 -> 192.168.88.90

2.4.5-p1 rule example:

```
rdr on vtnet2 proto tcp from any to 172.16.16.52 port 2000 -> 192.168.88.90
rdr on { vtnet0 vtnet2.23 enc0 openvpn } proto tcp from any to 172.16.16.52 port 2000 -> 192.168.88.90
```

```
pass  in  quick  on $SYNC inet proto tcp  from any to 192.168.88.90 port 2000 tracker 1614440714 flags S/SA keep state  label "USER_RULE: NAT "
```

2.5+:

```
rdr on vtnet2 inet proto tcp from any to 172.16.16.52 port 2000 -> 192.168.88.90
rdr on { vtnet0 vtnet2.23 enc0 openvpn } inet proto tcp from any to 172.16.16.52 port 2000 -> 192.168.88.90
pass  in  quick  on $SYNC inet proto tcp  from any to 192.168.88.90 port 2000 tracker 1614440714 flags S/SA keep state  label "USER_RULE: NAT "
```

there may be a pf bug

#9 - 03/08/2021 07:40 PM - Greg Hulands

Site to Site OpenVPN is broken for me in 2.5.0. The tunnel encryption is setup, but running openvpn at verbosity level 7, I see

```
router.myhomenetwork.homeip.net/aaa.bbb.ccc.ddd:39863 MULTI: bad source address from client [172.16.1.2], packet dropped
```

I'm using a 1:1 NAT rule.

```
binat on ovpns2 inet from 10.89.0.0/30 to any -> 172.17.1.0/30
```

This is the openvpn server config

```
dev ovpns2
verb 7
dev-type tun
dev-node /dev/tun2
writepid /var/run/openvpn_server2.pid
#user nobody
#group nobody
script-security 3
daemon
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
proto udp
auth SHA512
up /usr/local/sbin/ovpn-linkup
down /usr/local/sbin/ovpn-linkdown
multihome
tls-server
server-ipv6 fd62:dc41:d1a0:beef::/64
```

```
client-config-dir /var/etc/openvpn/server2/csc
ifconfig 10.89.0.1 10.89.0.2
ifconfig-ipv6 fd62:dc41:d1a0:beef::1 fd62:dc41:d1a0:beef::2
tls-verify "/usr/local/sbin/ovpn_auth_verify tls 'exit-vpn.myhomenetwork.homeip.net' 2"
lport 1194
management /var/etc/openvpn/server2/sock unix
max-clients 1
route 172.16.1.0 255.255.255.0
capath /var/etc/openvpn/server2/ca
cert /var/etc/openvpn/server2/cert
key /var/etc/openvpn/server2/key
dh /etc/dh-parameters.4096
tls-crypt /var/etc/openvpn/server2/tls-crypt
ncp-disable
cipher AES-256-GCM
allow-compression no
persist-remote-ip
float
```

```
Routing tables

Internet:
Destination        Gateway            Flags     Netif Expire
default            xxx.yyy.zzz.1      UGS         em0
10.89.0.1          link#7             UHS         lo0
10.89.0.2          link#7             UH       ovpns2
127.0.0.1          link#3             UH          lo0
172.16.1.0/24      10.89.0.2          UGS      ovpns2
xxx.yyy.zzz.0/24   link#1             U           em0
xxx.yyy.zzz.183    link#1             UHS         lo0
192.168.11.0/24    10.89.0.2          UGS      ovpns2

Internet6:
Destination                       Gateway                       Flags     Netif Expire
default                           fe80::1%em0                   UG          em0
::1                               link#3                        UH          lo0
xxxx:yyyy::/64                    link#1                        U           em0
xxxx:yyyy::5                      fe80::1%em0                   UGHS        em0
xxxx:yyyy::f03c:91ff:aaaa:bbbb    link#1                        UHS         lo0
fd62:dc41:d1a0:beef::/64          link#7                        U        ovpns2
fd62:dc41:d1a0:beef::1            link#7                        UHS         lo0
fd62:dc41:d1a0:e3b4::11:1         fd62:dc41:d1a0:beef::2        UGHS     ovpns2
fe80::%em0/64                     link#1                        U           em0
fe80::f03c:91ff:aaaa:bbbb%em0     link#1                        UHS         lo0
fe80::%lo0/64                     link#3                        U           lo0
fe80::1%lo0                       link#3                        UHS         lo0
fe80::d0ee:e8:cb6:be3e%ovpns2     link#7                        UHS         lo0
```

I'm currently installing 2.4.5 to compare the pf rules and will update with a diff later.

#10 - 03/09/2021 01:48 PM - Jim Pingle

- Target version changed from CE-Next to 2.5.1

#11 - 03/09/2021 01:48 PM - Jim Pingle

- Assignee set to George Neville-Neil

gnn is taking a look at this to see if he can track it down.

#12 - 03/12/2021 10:50 AM - Greg Hulands

Just to update. The nat rule on 2.4.5p1 for 1:1 Nat is

```
binat on ovpns2 from 10.89.0.0/30 to any -> 172.17.1.0/30
```

no inet

#13 - 03/12/2021 12:38 PM - Jim Pingle

- Subject changed from Port forward works only on interface with default gateway, does not work for alternative wans to State matching problem with reponses to packets arriving on non-default WANs

Updating subject for release notes.

Also made it more general since this can affect more than port forwards.

#14 - 03/12/2021 10:31 PM - Eduard Rozenberg

Sounds like this issue might be causing my problem but I can't tell 100% from the description.

One of our sites has a single firewall and multiwan (WAN1, WAN2, WAN3).
LAN is set up to route to GW group (WAN1-Tier1, WAN2-Tier1, WAN3-Tier2)

After updating firewall 2.4.5 to -> 21.02-RELEASE-p1, cannot SSH from outside to a machine on that LAN using WAN2 or WAN3 IP addresses. Only works connecting to IP's on WAN1 (default WAN).

Trying to SSH from outside to WAN2 or WAN3 IPs shows rejected traffic such as ">WAN2 23.45.67.89(22) -> 67.89.12.34(56123)" and the Easy Rule it suggests adding to WAN2 or WAN3 is nonsensical (and didn't help when I added it just to see what happens).

#15 - 03/16/2021 03:27 PM - James Blanton

Sounds like it may be related to my issue as well (#11630). It was working normally on my daily build from January during testing, but it was broken with the release of 2.5/21.02.

#16 - 03/16/2021 07:11 PM - Rick Strangman

I have the same problem with 21.02. No VPN's just straight multi-wan. WAN2 (non-default) responds to a ping and works outbound fine. When a inbound NAT is performed it hits the rule, the NAT rule passes it to the relevant server and the server just does not get its traffic back out. Serious issue.

#17 - 03/22/2021 08:48 AM - Kristof Provost

I've so far been unable to reproduce this problem.
It's possible that I'm missing some relevant factor in my setup.

Is everyone who's affected using PPPoE for at least one of their WAN interfaces?
Can an affected user share a backup of their configuration? Perhaps I'll spot what I'm missing to reproduce the issue.

#18 - 03/22/2021 08:54 AM - Grzegorz Krzystek

- File config-castor.ninex.info-20210322144941.xml added

#19 - 03/22/2021 11:45 AM - Kristof Provost

Thanks. I've not immediately spotted anything suspect in there.

However, it appears that all reports of this issue involve PPPoE WAN, and the pfsense route-to.diff patch treats point-to-point interfaces as special. My current hunch is that it PPP is going to prove to be a required factor to trigger this bug. I'm currently extending my setup to include one PPPoE WAN.

#20 - 03/22/2021 04:43 PM - Rick Strangman

- File config-pfsense.netech.local-20210321101619.xml added

I am not using PPPOE. Both WANs are DHCP. My config attached.

#21 - 03/23/2021 05:22 AM - Kristof Provost

With a PPPoE setup I still can't reproduce the problem. Along with the latest report that's fairly strong evidence that my hunch was wrong.

Unfortunately I'm running out of ideas. Without a reproduction scenario I don't think I can fix this.

#22 - 03/23/2021 05:33 AM - Grzegorz Krzystek

Kristof Provost wrote:

> With a PPPoE setup I still can't reproduce the problem. Along with the latest report that's fairly strong evidence that my hunch was wrong.
>
> Unfortunately I'm running out of ideas. Without a reproduction scenario I don't think I can fix this.

Jim was able to reproduce.
steps are easy:
2 wans (WAN +WAN2), on booth do port forward , like ssh -> box in lan.
With failover , primary router set on PFsense box to WAN
now from outside try to ssh to WAN2 ip address, will timeout, but to WAN will pass (ssh from outside network)
now change default router on pfsense to WAN2. you will get oposite result wan2 will pass , wan will timeout.

if you wish i can provide you access to affected system.

#23 - 03/23/2021 05:44 AM - Grzegorz Krzystek

What is funny is it need to be related with routing.
reflection nat works. this is impacting only when connection came from outside.

#24 - 03/23/2021 07:44 AM - Kristof Provost

Yes, that's the setup I have, and I'm unable to reproduce the problem. The port forwarding just work on both WAN and WAN2, no matter which WAN has the default route.

It might be helpful to be able to observe an affected machine, yes, assuming that it's safe to experiment with.

#25 - 03/23/2021 07:49 AM - Grzegorz Krzystek

please check your mailbox ;)

#26 - 03/23/2021 08:34 AM - Svein Wisnaes

Netgate XG-1537

21.02-RELEASE-p1 (amd64)
built on Mon Feb 22 09:39:51 EST 2021
FreeBSD 12.2-STABLE

2 x WAN with static IP

2 x LAN and 4 x VLANs

Server1 on LAN1
Server2 on LAN2

WAN2/GW2 is set as default. LAN1 has a FW rule to send all traffic out through WAN1/GW1.

Routing has been set up from WAN2/GW2 to LAN2 to a Server2. It works fine.
Routing has been set up from WAN1/GW1 to LAN1 to a Server1 and it is not working.

If I change default gateway to WAN1/GW1, the routing for WAN1 to LAN1 works just fine. But now the other one is not working anymore.

What previous version did this work in? What is the estimated time for a fix?

#27 - 03/23/2021 08:38 AM - Grzegorz Krzystek

last known working version is 2.4.5p1

No ETA on this, nor known workaround yet.

#28 - 03/23/2021 09:57 AM - Kristof Provost

Thanks for that.

The only progress I can report so far is that this demonstrates that the initial SYN arrives and is redirected as expected. `netstat -an` shows the expected addresses, in state SYN_RCVD. That would imply that the SYN+ACK is being sent, but as that's never seen on the link we can conclude that that packet is being dropped along the way.

The counters on the `pass in quick on pppoe0 reply-to (pppoe0 172.16.220.2) inet proto tcp from any to 127.0.0.1 port = ssh` rule seems to suggest that the SYN+ACK packet is also being handled by the pf, but I don't understand where it's getting dropped.

I'm trying to think of further debugging we can do to narrow this down further.

#29 - 03/23/2021 11:15 AM - Gerald Drouillard

I can concur that with 2 Wan Interfaces (different subnet in our case), with DMZ and LAN networks that traffic coming in WAN2 will not work. It worked with the previous version and the upgrade broke it. We had to change our DNS entries to use only WAN1 for inbound traffic. We are not using PPPOE.
Let me know what we can do to help.

#30 - 03/24/2021 07:32 AM - Svein Wisnaes

Grzegorz Krzystek wrote:

> last known working version is 2.4.5p1
>
> No ETA on this, nor known workaround yet.

What is the best way to install that version? Will it work choosing it under update and try installing? Or do we need to download and prepare something? As far as I have heard, the Netgate appliances have a special setup?

#31 - 03/24/2021 01:59 PM - Kris Phillips

Svein Wisnaes wrote:

> Grzegorz Krzystek wrote:
>
> > last known working version is 2.4.5p1
> >
> > No ETA on this, nor known workaround yet.
>
> What is the best way to install that version? Will it work choosing it under update and try installing? Or do we need to download and prepare something? As far as I have heard, the Netgate appliances have a special setup?

You can open a ticket with the support team and they will provide you with an image to burn to a USB key that has the recovery firmware.

#32 - 03/25/2021 05:01 PM - Kris Phillips

Testing with the following on amd64:

1. Created Port Forward from WAN address to internal and WAN2 set as default gateway: Works
2. Created 1:1 NAT for IP Alias VIP on WAN subnet to internal and WAN2 set as default gateway: Works
3. Created Port Forward from IP Alias VIP on WAn subnet to internal and WAN set as default gateway: Works
4. Created all three above with LAN to WAN rule configured to use a Gateway Group with WAN1 as primary and WAN2 as secondary and the firewall's default gateway as WAN2: Works

I'm unable to reproduce this issue. There must be very specific configuration characteristics to this bug that is outside of my above testing.

#33 - 03/25/2021 05:11 PM - Jordan Bradley

My setup is that I'm trying to do port forwarding on an openvpn client interface in order to forward a reserved port to nginx on a test machine. Packet capture shows in incoming connection on the VPN interface but nginx never gets the connection and thus the connection times out.

#34 - 03/25/2021 07:08 PM - David Socha

Kris,

I can reliably reproduce this bug on my systems. We are running 2 C2758s in a MultiWAN / HA config. We set our external DNS records to only point to the connection that is our default wan gateway to fix this. NAT is setup as Port Forward, with some outbound NAT. I have config backups from both of the firewalls in the config immediately before I upgraded from 2.4.5 to 21.02-p1, as well as backups that I just took. The backups are full backups of the system, and are too big to upload to this post. Please let me know if you would like me to send them in, or if you want to hop on to our systems and see the bug live.

Thanks,

David

#35 - 03/25/2021 08:10 PM - Kris Phillips

Kris Phillips wrote:

> Testing with the following on amd64:
>
> 1. Created Port Forward from WAN address to internal and WAN2 set as default gateway: Works
> 2. Created 1:1 NAT for IP Alias VIP on WAN subnet to internal and WAN2 set as default gateway: Works
> 3. Created Port Forward from IP Alias VIP on WAn subnet to internal and WAN set as default gateway: Works
> 4. Created all three above with LAN to WAN rule configured to use a Gateway Group with WAN1 as primary and WAN2 as secondary and the firewall's default gateway as WAN2: Works
>
> I'm unable to reproduce this issue. There must be very specific configuration characteristics to this bug that is outside of my above testing.

Additional testing:

Configured an SG-1100 with two WANs and tried the same testing as above thinking this may be an issue with VLANs and logical ports since a lot of mentions of PPPoE and devices with switch ports having issues. Unfortunately this also worked fine and I wasn't able to reproduce. Ran through the same testing as mentioned previously.

#36 - 03/25/2021 09:19 PM - Rick Strangman

The issue is:
1. 2 x WAN, WAN1 & WAN 2, both DHCP
2. WAN1 set as default gateway
3. Both WANs have identical NAT rules
4. WAN1 & WAN2 work fine outbound
5. WAN1 NAT to internal works fine
6. WAN2 NAT to internal passes the rule to the internal but no response back
7. I cannot test switching gateways as this is a production machine

#37 - 03/27/2021 04:28 AM - DRago_Angel [InV@DER]

Just wanted to add that this issue also impact IPv6 NPt with multiwan, please check this as well when fix will be at qa stage. I mentioned that in https://redmine.pfsense.org/issues/11188 and https://forum.netgate.com/topic/159354/pfsense-2-5-0-a-20201127-0650-nat-issues/ here. Thanks.

#38 - 03/27/2021 11:30 PM - Rick Strangman

- File LAN_to_Bad_WAN.cap added

I attach a pfsense packet capture on the LAN side from the bad WAN2. You can see that the initial SMTP request comes in, the SMTP server responds, but this response never makes it back out WAN2. The remote end continues with retransmission packets which the LAN SMTP server sees and again responds. This happens until to connection is dropped by the remote end.

#39 - 03/28/2021 12:23 AM - Craig Leres

I believe I'm also encountering this issue, at least a google for "pfsense rdr not working after upgrade" brought me here.

My configuration is way too complicated to post but I do have a spare SG-1100 so if this drags on I might try to build a simple config that shows the issue.

I have 7 openvpn tunnels, two are server, the rest clients. Many of these are pairs of IPv4+IPv6 tunnels going to the same destinations. I use manual outbound NAT rule generation.

Here's a example that was working with 2.4 but not 21.02 I was poking at tonight. My pfsense box is the openvpn client and the tun devices are assigned 10.4.0.0/24 addresses. On the remote server (10.4.0.1) I have a rdr that redirects tcp connections to port 22/ssh to the pfsense end of the tunnel (10.4.0.5) on port 9022. The pfsense box has a rdr that matches this and sends to local host on the lan (172.0.0.2) port 22/ssh. Tcpdump on 172.0.0.2 shows the tcp packets arrive and the responses from sshd are sent back. But "tcpdump -n -i pflog0" (my firewall config always logs dropped packets) shows the response being dropped:

```
rule 5/0(match): block out on ovpnc3: 10.4.0.5.9022 > 203.0.113.100.40984: Flags [S.], seq 576326524, ack 1032
881125, win 65535, options [mss 1460,nop,wscale 9,sackOK,TS val 747951710 ecr 2735271947], length 0
```

I can see the the automatic firewall rule created on behalf of rdr rule that allows 203.0.113.100.* > 10.4.0.5.9022 has "state type" keep which is how I believe this traffic used to make it back down ovpnc3. But for some reason the rule is not matching the return traffic.

I've added various explicit firewall rules but nothing I've tried matches 10.4.0.5.9022 > 203.0.113.100.*.

#40 - 03/29/2021 03:16 AM - Kristof Provost

Rick Strangman wrote:

> I attach a pfsense packet capture on the LAN side from the bad WAN2. You can see that the initial SMTP request comes in, the SMTP server responds, but this response never makes it back out WAN2. The remote end continues with retransmission packets which the LAN SMTP server sees and again responds. This happens until to connection is dropped by the remote end.

Thanks Rick. That confirms my own observations.

#41 - 03/30/2021 02:48 PM - Renato Botelho

- Assignee changed from George Neville-Neil to Kristof Provost

#42 - 03/30/2021 04:00 PM - Jim Pingle

- Project changed from pfSense to pfSense Plus

- Category changed from Rules / NAT to Rules / NAT

- Target version changed from 2.5.1 to 21.02.2

- Affected Version deleted (2.5.0)

A few notes:

- This only appears to affect pfSense Plus, not CE, which explains why some people cannot reproduce the problem.
- This happens on every architecture of pfSense Plus I have tried (amd64, arm64, armv7) on hardware (7100, 3100, 1100, 1000, and others) as well as VMs.
- An identical VM with an identical configuration on Plus and CE will work on CE and fail on Plus.
- The simplest test case is a port forward on both WANs for port 222 to 127.0.0.1 port 22.
- The client making test connections must be on a remote subnet -- not shared with either WAN directly.
- The port forward always works on the WAN with the default gateway, always fails on the WAN that isn't default.
- Changing the default gateway changes which WAN will work vs which one will fail -- as above, the default gateway interface always works.
- No differences in rules.debug between CE and Plus.
- Firewall log shows the SYN+ACK response blocked in the outbound direction on the affected WAN, as if it did not match the existing state.

I have status outputs from Plus and CE on the test VM in question.

#43 - 03/30/2021 04:08 PM - Jordan Bradley

I'm using community edition and this bug is affecting me.

#44 - 03/30/2021 04:10 PM - Jim Pingle

Jordan Bradley wrote:

> I'm using community edition and this bug is affecting me.

Based on your description above it's not likely the same bug. The symptoms are not the same. Post on the forum to diagnose it further.

#45 - 03/30/2021 05:10 PM - Rick Strangman

I can confirm that it does not occur in CE v5.0. I had the config operational before I migrated to Netgate x7100 with 21.02

#46 - 03/31/2021 12:47 PM - Grant Derhofer

- File pfSense.PNG added

I am trying to reproduce with CE my scenario in a virtual environment and was having issues, good to know it doesn't occur on CE. My 4860 is running pfSense+ and does have the issue.

My config overview:
WAN is a DHCP
Multiple port forwards from WAN to web and other for my own use (Owncloud/etc)
OpenVPN Client to PIA for whole house secure internet

After upgrading from 2.4.5 to 21.02, my NATs no longer work when the OpenVPN client is enabled, but work fine when disabled.

I pretty much have the CE environment up (just a few nuances with the OpenVPN I built in it to work out where connected clients can't reach anything) and not sure if there is a way to convert a CE to a pfSense+ version to see if I can reproduce the issue. It is fully self-contained using 4 pfSense VMs (one to ack as the "internet", a VPN server, 2.4.5, and 2.5.0) with 4 Ubuntu VMs on each level with a web server to test connectivity in/out.

#47 - 04/03/2021 07:24 AM - Kristof Provost

I've reproduced the issue, and believe I have a fix.
I'm still trying to work out why it didn't happen on CE though.

#48 - 04/05/2021 01:31 PM - Renato Botelho

- Status changed from New to Feedback

- % Done changed from 0 to 100

Fix was pushed to FreeBSD and cherry-picked to FreeBSD-src on commit 4fd4e2b70189

#49 - 04/06/2021 05:05 PM - Grzegorz Krzystek

Renato Botelho wrote:

> Fix was pushed to FreeBSD and cherry-picked to FreeBSD-src on commit 4fd4e2b70189

works on 21.02.2-RC
thank you

#50 - 04/06/2021 05:17 PM - Grzegorz Krzystek

to be more precise tested on build 21.02.2.r.20210405.1121

on booth wans port forward works now as expected.
Good Job. @Kristof Provost

#51 - 04/06/2021 05:24 PM - Rick Strangman

So is this build different that what shows up in System->Updates?

#52 - 04/06/2021 05:30 PM - Grzegorz Krzystek

I tested it on RC update channel
currently running 21.02.2.r.20210406.1302
and port forward works as expected. on booth WANS.
so all is fine, we should expect this fix go prod with 21.02.2 upcomming release.

#53 - 04/07/2021 05:07 AM - Rick Strangman

I can confirm the issue has been resolved. Explanation please.

#54 - 04/07/2021 05:10 AM - Grzegorz Krzystek

@Rick Strangman

> Updated by Renato Botelho 1 day ago
> ...
> Fix was pushed to FreeBSD and cherry-picked to FreeBSD-src on commit 4fd4e2b70189

#55 - 04/07/2021 08:03 AM - Renato Botelho

- Status changed from Feedback to Resolved

#56 - 04/08/2021 05:49 PM - Eduard Rozenberg

Working fine for me now after update to 21.02.2.r.20210406.1302
Now once again able to connect to the network from the outside over WAN2 and WAN3, not just WAN1.

Looks like the explanation is here:
https://github.com/pfsense/FreeBSD-src/commit/4fd4e2b70189485f6a277260eba24ec4ae63159c

But no clue why 2.5 never had this problem (assuming reports stating that are correct).

#57 - 04/14/2021 07:36 AM - Jim Pingle

Some reports that this is happening on CE now, but not Plus. See #11805

Keeping this one closed since it was specific to Plus and it is solved.

#58 - 04/16/2021 04:18 AM - DRago_Angel [InV@DER]

Updated to 21.02.2-RELEASE and NPt still not works on non-primary WAN so issue resolved not fully.

#59 - 04/16/2021 10:18 AM - Kristof Provost

DRago_Angel [InV@DER] wrote:

> Updated to 21.02.2-RELEASE and NPt still not works on non-primary WAN so issue resolved not fully.

Can you provide some details on both your setup and precises what does not work?

#60 - 04/19/2021 04:33 AM - DRago_Angel [InV@DER]

Don't know what details exactly you like, will provide that I can publicly, but if you need more details (e.g. status.php) lets continue in email.
So I have:

- 2 WANs for IPv4 and both WANs have own GIF interface for tunnelbroker.net (e.g. 2001:ff:a::/48 and 2001:ff:b::/48).
- Local clients get IPs from main IPv6 tunnel subnet (e.g. 2001:ff:a::1).
- I have NPt that nating all /48 subnet from main IPv6 tunnel 2001:ff:a::/48 to second IPv6 tunnel 2001:ff:b::/48 subnet.
- Outgoing connections works fine if at least one gateway is UP.
- Incoming connections works only for active IPv6 tunnel IPs, (e.g. 2001:ff:a::1), but not works on any not active IPv6 (e.g. 2001:ff:b::1) while actually gateway is UP.

#61 - 04/20/2021 06:49 AM - Kristof Provost

Please post your full configuration file (censor any passwords / keys) or e-mail it to me at kprovost@netgate.com.
Your /tmp/rules.debug may also be helpful.

#62 - 04/20/2021 01:23 PM - DRago_Angel [InV@DER]

<removed>

#63 - 04/20/2021 01:55 PM - DRago_Angel [InV@DER]

Hi Kristof,

Sorry, my test was been incorrect, NPt actually works on 21.02.2-RELEASE (amd64).
My firewall rule was wrong, I put allow rule DST: 2001:ff:b::1, but correct value was 2001:ff:a::1 on WAN02 where IPs are 2001:ff:b::1. This due to logic of IPFW - in end it real 2001:ff:a::1 and I forget about it.

#64 - 04/27/2021 08:39 PM - Jim Pingle

This issue is for Plus only. The issue for CE is #11805

Files

config-castor.ninex.info-20210322144941.xml	139 KB	03/22/2021	Grzegorz Krzystek

config-pfsense.netech.local-20210321101619.xml	1.12 MB	03/22/2021	Rick Strangman
LAN_to_Bad_WAN.cap	1.11 KB	03/28/2021	Rick Strangman
pfSense.PNG	24.7 KB	03/31/2021	Grant Derhofer