pfSense - Feature #7727

uPnP fails to properly give out subsequent reservations when multiple gaming systems are playing the same game/using the same port.

07/26/2017 11:46 AM - Anonymous

Status:	In Progress	**Start date:**	07/26/2017
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	0%
Category:	uPNP	**Estimated time:**	0.00 hour
Target version:	CE-Next		
Release Notes:	Default		

Description

It's a bug with pfsense, at least in my eyes (nearly 15 years experience in IT and am a senior security engineer with a fortune 500 company). You currently cannot have 2 systems, whether console or gaming PC playing the same game at the same time using pfsense. The second client will always fail to connect. I have done everything you are supposed to do:Static outbound ports, uPnP ACL, firewall rules, NAT reflection. I even hired a freelancer with pfsense experience going back to when it was monowall. He took 10 minutes to look at my config and told me that it looked exactly how it was supposed to look. He then did his own troubleshooting and came to the exact conclusion that I did. uPnP is broken in pfsense 2.4.

Just to prove a point I plugged in my netgear r8500, booted it up, updated its firmware and restored defaults. Upon the subsequent reboot, the 2 clients picked up uPnP reservations immediately (unlike pfsense where it takes 30+ seconds to get the one that does eventually pickup) and both reported back with open nat. I was able to join the same lobbys with both clients and play together for extended periods.

History

#1 - 07/26/2017 11:48 AM - Anonymous

the game in question is "For Honor", but im pretty sure it affects any game that uses peer to peer matchmaking. There is also an issue with being the host, but that may be a hard limitation that cannot be overcome, unsure.

#2 - 04/07/2019 10:38 PM - Shane Angelo

Hi All,

I have experienced the same issue as reported in the bug descrip.

I have also discovered when searching the net for a solution that many other folks have too, all without solutions. I have followed the guides available which covers the configurations listed by the original bug descrip and gives me open NAT as reported on all the xbox consoles (3 in total).

However, when playing multiplayer from with LAN network using the same game, the second and subsequent xboxes to be connected always fails to connect to the game lobby.

With only one xbox there is no issue connecting and playing.

When playing different game titles at the same time there are no issues connecting and playing

Access to the lobby fails only for the second connected xbox console when playing the same title concurrently.

As a test, I replaced the pfsense firewall with an off the shelf generic router with uPnP enabled and immediately all xboxes are able to connect. No other settings were changed on the network.

I have a basic knowledge, but I am more than happy to help do my part to help resolve this issue. I'd rather not replace pfsense for all the other benefit it brings on account of the occasional xbox game with my son.

Seen this on Call of Duty WW2, Titanfall 2 and now Apex Legends. I have no doubt that it affects other titles too.

As a workaround I am going to try putting the second console in a DMZ.

Thanks,
CV8R

#3 - 08/13/2019 09:50 AM - Jim Pingle

- Tracker changed from Bug to Feature

- Project changed from pfSense Packages to pfSense

- Category set to uPNP

- Affected Version deleted (2.4.x)

- Affected Architecture deleted (amd64)

AFAIK This is because last I looked, miniupnpd doesn't support its "masquerade" options on FreeBSD/pf like it does on Linux/netfilter. When it is set to masquerade, it sets up an outbound (snat/source nat) mapping to maintain a static source port for the same port requested by the client. Without that, you only get inbound NAT, and if you setup static port on outbound NAT you're only likely to get a single console working as expected.

I doubt there is anything we can do here unless someone adds support for that to miniupnpd

#4 - 03/29/2020 10:45 PM - Russell Graville

Jim Pingle wrote:

> AFAIK This is because last I looked, miniupnpd doesn't support its "masquerade" options on FreeBSD/pf like it does on Linux/netfilter. When it is set to masquerade, it sets up an outbound (snat/source nat) mapping to maintain a static source port for the same port requested by the client. Without that, you only get inbound NAT, and if you setup static port on outbound NAT you're only likely to get a single console working as expected.
>
> I doubt there is anything we can do here unless someone adds support for that to miniupnpd

I see it may have been updated in miniupnpd for FreeBSD. How soon can this me imported into pfsense?:

https://github.com/miniupnp/miniupnp/blob/master/miniupnpd/Changelog.txt
$Id: Changelog.txt,v 1.458 2020/03/29 09:07:37 nanard Exp $

2020/03/29:
Fix FreeBSD build

#5 - 03/30/2020 11:08 AM - Jim Pingle

That isn't relevant to this feature. It's a different FreeBSD issue. I don't see anything about masquerade being added to pf.

#6 - 04/25/2020 12:29 PM - Marc 05

Jim Pingle wrote:

> That isn't relevant to this feature. It's a different FreeBSD issue. I don't see anything about masquerade being added to pf.

Looks like there is some progress on this:
"netfilter: addmasqueraderule() even if internal/external ports are the same"
https://github.com/miniupnp/miniupnp/commit/e49d44f700355552c45a95c1e067e4a815479557

I hope this gets patched in as a hotfix or something soon - many people have been waiting on this for a long time!

#7 - 04/26/2020 11:55 AM - Marc 05

If it ends up working for you, would you provide it in a way that I could apply it using the System Patches package? Would be good to update this thread as well https://github.com/miniupnp/miniupnp/issues/413

#8 - 04/26/2020 12:05 PM - Jim Pingle

Marc05 M wrote:

> Looks like there is some progress on this:
> "netfilter: addmasqueraderule() even if internal/external ports are the same"
> https://github.com/miniupnp/miniupnp/commit/e49d44f700355552c45a95c1e067e4a815479557
>
> I hope this gets patched in as a hotfix or something soon - many people have been waiting on this for a long time!

That still isn't adding masquerade support for PF. It's not related.

Joel Samson wrote:

> Kind of ridiculous this has has been open for nearly 3 years and nothing, I am in the process of setting up my build server to compile this above and manually install it over the pfsense base version using the instructions found here: https://docs.netgate.com/pfsense/en/latest/packages/installing-freebsd-packages.html?highlight=pkg as I no longer have time to wait, either a solution is applied or I move back to Untangle.

You need to advocate to miniupnpd for them to add support for masquerade to their PF code. It's a missing feature in miniupnpd, not much we can do about that.

#9 - 04/26/2020 12:50 PM - Joel S

Jim Pingle wrote:

> Marc05 M wrote:

> > Looks like there is some progress on this:
> > "netfilter: addmasqueraderule() even if internal/external ports are the same"
> > https://github.com/miniupnp/miniupnp/commit/e49d44f700355552c45a95c1e067e4a815479557
> >
> > I hope this gets patched in as a hotfix or something soon - many people have been waiting on this for a long time!
>
> That still isn't adding masquerade support for PF. It's not related.
>
> Joel Samson wrote:
>
> > Kind of ridiculous this has has been open for nearly 3 years and nothing, I am in the process of setting up my build server to compile this above and manually install it over the pfsense base version using the instructions found here: https://docs.netgate.com/pfsense/en/latest/packages/installing-freebsd-packages.html?highlight=pkg as I no longer have time to wait, either a solution is applied or I move back to Untangle.
>
> You need to advocate to miniupnpd for them to add support for masquerade to their PF code. It's a missing feature in miniupnpd, not much we can do about that.

To be fair, that is already done as found here: https://github.com/miniupnp/miniupnp/issues/413 and the change discribed above does seem to be related.
Otherwise, if you have another feature missing not identified in that Github change for miniupnpd, then YOU should request the change to them, as clearly it's an open request here for as long as 3 years and you have still not reached out to the vendor?

Sounds like some slacking on some side. Defiantly not the client side of your software lmao.

#10 - 04/26/2020 12:58 PM - Jim Pingle

Nothing on that bug report mentions pf, all of the example commands are for Linux. It may be about masquerade mode issues in general but it doesn't appear to be specifically doing anything for pf.

#11 - 04/26/2020 01:04 PM - Marc 05

Hi Jim. Given you likely understand the issue much better than I, would you help me in making the request necessary to resolve this? What exactly should be requested - would it just be creating a feature request in the miniupnp repo asking for "add support for masquerade to their PF code" and nothing else?

#12 - 04/26/2020 01:11 PM - Joel S

Marc05 M wrote:

> Hi Jim. Given you likely understand the issue much better than I, would you help me in making the request necessary to resolve this? What exactly should be requested - would it just be creating a feature request in the miniupnp repo asking for "add support for masquerade to their PF code" and nothing else?

I would agree with this. I am willing to submit the request on Github for pfsense specific issues.
But we need to better understand what to request, what support needs to be added specifically for PFsense?

While those changes are specific to Linux, PFsense is FreeBSD based (Unix-based) and you would expect the feature to be added/migrated fairly easily if we can get a clear picture of what needs to be added/ported to the pfsense (unix-based) version.

Thanks,

#13 - 04/27/2020 09:35 AM - Jim Pingle

Marc05 M wrote:

> Hi Jim. Given you likely understand the issue much better than I, would you help me in making the request necessary to resolve this? What exactly should be requested - would it just be creating a feature request in the miniupnp repo asking for "add support for masquerade to their PF code" and nothing else?

I'm not sure what detail they would need beyond "Add masquerade feature to pf support" or something along those lines. Currently the masquerade references are all inside their netfilter code which is only on Linux.

The request is not specific to pfSense, but pf in general (So, primarily FreeBSD and OpenBSD).

#14 - 04/27/2020 11:25 AM - Jim Pingle

I don't see anything like that in the linked reference. Only confirmation that the issue/commit only apply to netfilter.

And no, an update for miniupnpd wouldn't be in the package manager. It's a base system package and would only be updated with a new release.

#15 - 04/27/2020 12:00 PM - Jim Pingle

Joel S wrote:

> He specifically comments that "I'm stupid, e49d44f is only for netfilter :(it will change nothing for pf :(I don't know how I forgot this issue was about netfilter in the 1st place."
>
> Obviously, he will ask for a new bug report outside of the netfilter one, or simply make the commit change from that existing bug now that he realizes his mistake that the changes are only for linux and not Pfsense.

I saw that, but nothing in that implies any action for pf. Only that the issue is about netfilter. There is no masquerade code at all for pf, they'd have to completely port over the feature. You're reading an awful lot between the lines there that isn't even implied. Kudos to you for being optimistic, but I'm not holding my breath on it happening any time soon.

> I hope you generally understand that once this is done, this issue then falls directly on you to update the package on the base system if it's not available as an update.
> Not sure why it sounds like you keep trying to redirect this, it's coming your way either way within a few days at most (Likely Thursday it will be resolved). At which point this thread will become the highlight, not: https://github.com/miniupnp/miniupnp/issues/413

When they have it in their code base and we know it works on FreeBSD+pf, it will find its way into a pfSense release. We redirect the issue to miniupnpd because they're the ones that need to add the feature first. It's entirely up to them, until they include it in a release.

#16 - 04/27/2020 12:21 PM - Marc 05

A bit off-topic:

It's funny that throughout all of the years, many people have encountered and posted about the issue in one way or another, and only in the last few days has there been any semblance of progress.

Thank you Joel for all of the follow-up, and please keep it up. It's appreciated, even if you are just copying and pasting.

Thank you Jim for telling us what to do :D No doubt there are plenty of other things in need of attention. I hope this issue finally gets its spotlight after being background noise for so long.

#17 - 05/09/2020 07:20 PM - Cameron O

Hi, I'm also interested in this issue and really glad to see there's an active effort to get it resolved. Thanks Joel, Marc, and Jim!

I'm posting because I think it may help myself and others to clearly understand the issue.
Based on comments in the linked Github issue, past forum posts, and how long this issue has been around, I think users have been at least a little confused about what *exactly* the problem is.

My understanding of NAT rules and other networking jargon is shaky, but am I correct in summarizing what's been said before like this?

- To easily allow multiple devices to play the same online games, pfsense needs to be able to create an inbound and outbound NAT rule for every UPnP port forward.
- The version of the uPnP library used by pfsense only allows creating inbound NAT rules.

Jim did sort of say as much in the beginning, I'm just not sure if my reading is correct.

Jim Pingle wrote:

> When it is set to masquerade, it sets up an outbound (snat/source nat) mapping to maintain a static source port for the same port requested by the client. Without that, you only get inbound NAT, and if you setup static port on outbound NAT you're only likely to get a single console working as expected.

"Masquerade" has been thrown around a lot in this thread, and it's pretty confusing, especially if the issue is more about having a two-way mapping.
nefilter's iptables MASQUERADE option just allows making an outbound NAT (SNAT) rule without specifying the public external IP address.
I can see why this is necessary since many users might have dynamic IP addresses, but it does look like pf can do the same thing—pulling an address from an interface (eth0 in this example).

IPTABLES
iptables -t nat -a POSTROUTING -s 1.2.3.4 -o eth0 -j MASQUERADE

PF
nat on eth0 from 1.2.3.4 to any -> (eth0)

So is the pf-based miniupnpd just missing some internal or API feature that's in the netfilter-based version or does pf itself actually not have a way to do what iptables does?
There's a big difference if this some functional gap between netfilter and pf or something of an oversight/backlogged feature in miniupnpd.

#18 - 05/10/2020 06:27 PM - Star Jesus

I bought the SG-3100 because I wanted to have the BiS router for epic gaming moments

Turns out one of the "features" of the wonderful pfsense software is that two PCs can't play Call of Duty at the same time together

What was supposed to be an epic moment is actually an epic fail

I spent my Trump bucks on this crap

#19 - 05/11/2020 09:19 AM - Jim Pingle

Cameron O wrote:

> So is the pf-based miniupnpd just missing some internal or API feature that's in the netfilter-based version

pf is capable of doing this kind of NAT, it's the same kind of NAT rules people set manually to make single consoles work (static port).

The problem is that miniupnpd doesn't have any pf code to set that up (no masquerade code for pf in miniupnpd)

#20 - 05/11/2020 09:22 PM - Joel S

Jim Pingle wrote:

> pf is capable of doing this kind of NAT, it's the same kind of NAT rules people set manually to make single consoles work (static port).
>
> The problem is that miniupnpd doesn't have any pf code to set that up (no masquerade code for pf in miniupnpd)

Marc05 M wrote:

> A bit off-topic:
>
> It's funny that throughout all of the years, many people have encountered and posted about the issue in one way or another, and only in the last few days has there been any semblance of progress.
>
> Thank you Joel for all of the follow-up, and please keep it up. It's appreciated, even if you are just copying and pasting.
>
> Thank you Jim for telling us what to do :D No doubt there are plenty of other things in need of attention. I hope this issue finally gets its spotlight after being background noise for so long.

Opened a new issue for this pf masquerade feature implementation at the dev's request, it can be found here:
https://github.com/miniupnp/miniupnp/issues/448
The other issue linked was cleaned up to keep it related to Netfilter, as expected though this is still moving, I was not surprised he asked for a new issue report as I mentioned above.
Maybe Jim can review the new issue created, and provide feedback on anything or any details missing which I can add :)

Thanks again all!
Happy to see this moving in the right direction finallllllyyyy!!!

#21 - 05/17/2020 07:40 PM - Joel S

Jim Pingle wrote:

> pf is capable of doing this kind of NAT, it's the same kind of NAT rules people set manually to make single consoles work (static port).
>
> The problem is that miniupnpd doesn't have any pf code to set that up (no masquerade code for pf in miniupnpd)

miniupnpd dev would like the following information from our setup:

the AddPortMapping() requests done
the subsequent pf rules created by miniupnpd
the ones that would be expected so the traffic flows properly and the game works on all xbox's

Which commands can I use to get the first 2 results? I can at least provide that to him to start.
As for the rules/flows to be expected, we may need to wait to see what is actually happening...

Thanks again guys.
Joel S.

#22 - 05/17/2020 07:52 PM - Joel S

Jim Pingle wrote:

> pf is capable of doing this kind of NAT, it's the same kind of NAT rules people set manually to make single consoles work (static port).
>
> The problem is that miniupnpd doesn't have any pf code to set that up (no masquerade code for pf in miniupnpd)

He also mentioned how it looks like pf used in pfSense is an old version as rdr-anchor are not used since OpenBSD 4.7 (2010)

#23 - 05/18/2020 03:20 AM - Thomas BERNARD

Hello, I'm miniupnp main author.

The user Joel S came from here to open an issue on https://github.com/miniupnp/miniupnp/issues/448

From the start he showed no understanding of the problem, just asking for "high priority" fixing of a bug he was unable to expose clearly.

He then became very disrespectful, requiring me to work on his problem and opening several duplicate issues.
In 15 years, I have not seen such disrespect behavior from a "bug reporter".

The pfSense community has given a lot to miniupnp over the years, that's a shame that today such a spoiled boy wastes our time.

To come back to the issue itself:
I have seen no detailed description of the problem (AddPortMapping requests from the consoles, the pf rules that are produced, etc.) but I guess it has something to do with the inability of miniupnp/pf to make "bidirectional port mappings" it is possible to do with netfilter : ie when there is a port mapping added for external port 1111 to internal port 2222. Outbound UDP packets from port 2222 are not forced to be translated to source port 1111.
If it is confirmed that is it the real issue here, and if someone is able to produce the pf rules needed, I will be able to implement it in miniupnp pf backend.
But I'm afraid it is a feature currently not available in pf.

The static-port option to nat in pf just works for mapping with same external and internal port, so that source port 2222 is kept and not mapped to a random port.

Regards,

Thomas Bernard

#24 - 05/18/2020 07:16 AM - Joel S

Thomas BERNARD wrote:

> Hello, I'm miniupnp main author.
>
> The user Joel S came from here to open an issue on https://github.com/miniupnp/miniupnp/issues/448
>
> From the start he showed no understanding of the problem, just asking for "high priority" fixing of a bug he was unable to expose clearly.

No, I fully understand the problem. In-fact, you show zero understanding of the problem.
I don't understand the solution, there's a difference, which is why we came to you and Jim. Sadly after 3 years this is where we are, still no where with a solution.

> He then became very disrespectful, requiring me to work on his problem and opening several duplicate issues.
> In 15 years, I have not seen such disrespect behavior from a "bug reporter".
>
> The pfSense community has given a lot to miniupnp over the years, that's a shame that today such a spoiled boy wastes our time.
>
> To come back to the issue itself:
> I have seen no detailed description of the problem (AddPortMapping requests from the consoles, the pf rules that are produced, etc.) but I guess it has something to do with the inability of miniupnp/pf to make "bidirectional port mappings" it is possible to do with netfilter : ie when there is a port mapping added for external port 1111 to internal port 2222. Outbound UDP packets from port 2222 are not forced to be translated to source port 1111.
> If it is confirmed that is it the real issue here, and if someone is able to produce the pf rules needed, I will be able to implement it in miniupnp pf backend.
> But I'm afraid it is a feature currently not available in pf.
>
> The static-port option to nat in pf just works for mapping with same external and internal port, so that source port 2222 is kept and not mapped to a random port.
>
> Regards,
>
> Thomas Bernard

I would agree, I have never found someone so disrespectful to someone simply asking a question and/or for assistance. I love the name calling though, keep it up ;)
Doesn't bother me none, maybe that's all how your french coders are, all with their heads up their ass. Let me help you understand the issue.
"pfsense = toi et Jim corrigez le probleme"

I would love for you, no I would dare for you, to show me in the thread where I become disrespectful, at least until you told me to stop "wasting your time".
You and Jim has been wasting everyone's time from the start, if you could of simply talked to each-other as we requested, this wouldn't be an issue, but somehow the last time was in 2010, and since then you guys have been scared of each
other.

We simply want you two to stop ignoring it for over 3 years and start looking into it. Not a hard request.

Finally someone comes out from the darkness and crosses worlds, just had to piss him off a bit but that's fine. I don't care if what Jim is asking for isn't possible or if I don't understand. "THATS WHY YOUR HERE" :D
Now if you and Jim come to the conclusion this isn't a bug and everyone's configuration is wrong, at least it will become public knowledge. But I am pretty sure that is not the case ;) And you will need to prove it with all the users with the issue.

Get off your high horse bud, start being respectful to people asking you questions if you don't want to be shown disrespect, and don't kill the messenger, as you said all I do is copy and paste.
If it doesn't make sense, don't blame me. Blame the people asking me to bring it to you and telling us what to say (Jim).

But you don't deserve any respect for closing an issue early and shitting on the messenger. I am not impressed rolf. I'll be impressed when you do your job correctly and drop the god complex.

I swear you don't even read, you just slam the ban button, which sadly will not work.
Maybe if you and Jim and discussed this conversation 3 years ago, I wouldn't need to be a dick to get you to do stuff ;) But I don't mind it. It's moving ;)

Thanks,
Joel S.

#25 - 05/18/2020 09:26 AM - Jim Pingle

Joel,

Please stop. That kind of unhelpful dialog is unproductive and not welcome here, and is getting in the way of any meaningful discussion about solving the problem.

#26 - 05/18/2020 10:02 AM - Jim Pingle

Thomas BERNARD wrote:

> I have seen no detailed description of the problem (AddPortMapping requests from the consoles, the pf rules that are produced, etc.) but I guess it has something to do with the inability of miniupnp/pf to make "bidirectional port mappings" it is possible to do with netfilter : ie when there is a port mapping added for external port 1111 to internal port 2222. Outbound UDP packets from port 2222 are not forced to be translated to source port 1111.
> If it is confirmed that is it the real issue here, and if someone is able to produce the pf rules needed, I will be able to implement it in miniupnp pf backend.
> But I'm afraid it is a feature currently not available in pf.

OK, it's possible I'm misunderstanding what that does. I thought it setup an outbound rule which did the opposite of that, which translated outbound packets from the target to use the same port requested for UPnP. So for example:

S:12345->E:1111->C:2222
C:X->E:1111->S:Y (for new connections not replies on the state created for 1111->2222 since those would always reply from 2222->1111)

The pf rule for that would look something like this (client 10.6.0.11, ext addr 198.51.100.6, server 1.2.3.4):

```
nat on $WAN inet proto tcp from 10.6.0.11/32 to 1.2.3.4/32 -> 198.51.100.6/32 port 1111
```

Though I could see that failing in some cases if an overlapping state already exists for an inbound connection. It would only work for a single concurrent outbound connection to the same remote server, additional connections would fail since the external state portions would conflict.

From your last comment it sounds like what the netfilter rules do is to allow the replies to have a different source port on the way out, sort of like:

S:12345->E:1111->C:2222
C:2222->E:<some random port>->S:12345

I don't see a way to that in pf but I'm not sure I'm reading your statement properly. That doesn't seem to make sense, since the server would typically reject replies from a source port it wasn't actively communicating with.

Do you have an example set of netfilter rules/chains which shows the type of rules you are describing? That might help make it more clear since I'm fairly certain the problem is my (lack of) understanding.

#27 - 05/18/2020 10:39 AM - Thomas BERNARD

We have not enough precise details on the issue :
What AddPortMapping requests the XBoxes are doing and what traffic they are expecting.

It is important to note that everything applies only to UDP, not TCP.
My guess is that somehow they are expecting their outbound UDP traffic to be translated to a precise port.
When opening a port mapping with external port 1111 and internal port 2222.
If that is the Remote that sends the 1st packet to <public ip>:1111 everything works fine.
subsequent packets sent by the XBox to the remote will be translated with a source port of 1111 (existing "UdP connection")

But if that is XBox that sends the 1st packet to a remote host, the source port would either be kept as 2222 (static-port set) or a random one (non pre-existing "UDP connection")

With netfilter/iptables, we are using SNAT to force translation to the wanted source port.

#28 - 05/18/2020 11:26 AM - Thomas BERNARD

Joel S wrote:

> Jim Pingle wrote:
>
> > Joel,
> >
> > Please stop. That kind of unhelpful dialog is unproductive and not welcome here, and is getting in the way of any meaningful discussion about solving the problem.
>
> I will gladly stop now that progress is being made... Observing only for now. The fact is I had to do this, or we would be waiting another 2 years as you said, "You need to advocate to miniupnpd for them to add support for masquerade to their PF code" and we were tired waiting for nothing.
> It was helpful in that regard :)
>
> Thanks!
> Joel S.

I hope you will someday stop believing we are at your service. As far as I know, Jim is not your employee. He surely has more urgent issues than you and your friends not being able to play your favorite video games.

The fact that you believe that progress is being made just shows how deeply you don't understand the issue.
And the fact that you believe it is thanks to your aggressive behavior proves that you are not going to improve it anytime.

Such disrespect ruins the motivation of people involved in OSFS projects.

#29 - 05/18/2020 12:17 PM - Jim Pingle

I removed the irrelevant comments made after the warning and locked their account. Further comments unrelated to the technical nature of the issue alone will also be removed. Such comments only further erode the available time developers have to work on actual problems.

#30 - 05/18/2020 12:48 PM - Dakota Marshall

I've been watching this bug for the past 2 years and am excited that there is some traction on it. Though I'm very disappointed that it took such a sour turn. I would love to be of assistance on trying to figure out what exactly is going on. To note first I currently do not have an active PfSense box to test but I can likley get one up and running to help with any testing.

At this point, what is needed to try and further troubleshoot this issue? I will be more than happy to assist the best I can.

I do know that this issue is not isolated to Xbox if that matters. It applies to PC aswell, really any game service that uses matchmaking services over UDP. If it would help, I can setup 2 devices behind a pfsense router and attempt to have them connect to the same matchmaking service, I can do a full packet capture on all devices. Would there be any other details needed to try and troubleshoot?

#31 - 05/18/2020 02:59 PM - Thomas BERNARD

Dakota Marshall wrote:

> At this point, what is needed to try and further troubleshoot this issue? I will be more than happy to assist the best I can.
>
> I do know that this issue is not isolated to Xbox if that matters. It applies to PC aswell, really any game service that uses matchmaking services over UDP. If it would help, I can setup 2 devices behind a pfsense router and attempt to have them connect to the same matchmaking service, I can do a full packet capture on all devices. Would there be any other details needed to try and troubleshoot?

- We first need the AddPortMapping requests sent by the 2 (or more) devices. (you can capture traffic on the miniupnpd HTTP port).
  if you run miniupnpd in debug mode, it will also send theses info to syslog.

- then you can check which pf rules are created.
  depending on pf version, they are visible with
  pfctl -a miniupnpd -s rules
  and/or
  pfctl -a miniupnpd -s nat
  (if the miniupnpd version compiled for pfSense does use the "miniupnpd" anchor)

- then you can capture all traffic on your lan on the redirected port so we would know if game send packets to a remote host before it receives any from the same host.

After that we'll have confirmation of the diagnostics. But still no solution to make outgoing UDP packets translated with the right source port.

#32 - 05/18/2020 05:28 PM - Connor Ness

I can test this right now. I currently have two PCs unable to play Call of Duty together behind a pfSense 2.4.4-RELEASE-p3 box via upnp.

I have configured:

```
System -> Advanced -> Firewall & NAT -> Network Address Translation -> NAT Reflection mode for port forwards = "Pure NAT"
System -> Advanced -> Firewall & NAT -> Network Address Translation -> Enable automatic outbound NAT for Reflection = "True"
Firewall -> Aliases -> IP -> Firewall Aliases IP = [{"UPnPGames": ["192.168.1.48", "192.168.1.49", "192.168.1.50"]}]
Firewall -> NAT -> Outbound -> Outbound NAT Mode -> Mode = "Hybrid Outbound NAT rule generation"
Firewall -> NAT -> Outbound -> Mappings = [{"Enabled": True, "Interface": "WAN", "Source": "UPnPGames", "Source Port": "*", "Destination": "*", "Destination Port": "*", "NAT Address": > "WAN address", "NAT Port": "*", "Static Port": True, "Description": ""}]
Services -> UPnP & NAT-PMP -> UPnP & NAT-PMP Settings -> Enable = "True"
Services -> UPnP & NAT-PMP -> UPnP & NAT-PMP Settings -> UPnP Port Mapping = "True"
Services -> UPnP & NAT-PMP -> UPnP & NAT-PMP Settings -> Log Packets = "True"
Services -> UPnP & NAT-PMP -> UPnP & NAT-PMP Settings -> Default Deny = "True"
Services -> UPnP & NAT-PMP -> UPnP Access Control Lists -> ACL Entries = ["allow 0-65535 192.168.1.48/32 0-65535", "allow 0-65535 192.168.1.49/32 0-65535"]
```

My PC (.48) was able to connect with "Open" NAT. My brother's PC (.49) was unable; the game launches, then complains that it was unable to connect to the server. His only option from there is to quit to desktop.

Here is the response to `pfctl -a miniupnpd -s rules`:

```
pass in log quick on re0 inet proto udp from any to 192.168.1.48 port = 3074 flags S/SA keep state label "DemonwarePortMapping" rtable 0
pass in log quick on re0 inet proto udp from any to 192.168.1.49 port = 3074 flags S/SA keep state label "DemonwarePortMapping" rtable 0
pass in log quick on re0 inet proto udp from any to 192.168.1.49 port = 3074 flags S/SA keep state label "DemonwarePortMapping" rtable 0
pass in log quick on re0 inet proto udp from any to 192.168.1.49 port = 3074 flags S/SA keep state label "DemonwarePortMapping" rtable 0
pass in log quick on re0 inet proto udp from any to 192.168.1.49 port = 3074 flags S/SA keep state label "DemonwarePortMapping" rtable 0
```

Here is the response to `pfctl -a miniupnpd -s nat`:

```
rdr log quick on re0 inet proto udp from any to any port = 3074 keep state label "DemonwarePortMapping" rtable 0 -> 192.168.1.48 port 3074
rdr log quick on re0 inet proto udp from any to any port = 3148 keep state label "DemonwarePortMapping" rtable 0 -> 192.168.1.49 port 3074
rdr log quick on re0 inet proto udp from any to any port = 3194 keep state label "DemonwarePortMapping" rtable 0 -> 192.168.1.49 port 3074
rdr log quick on re0 inet proto udp from any to any port = 3155 keep state label "DemonwarePortMapping" rtable 0 -> 192.168.1.49 port 3074
rdr log quick on re0 inet proto udp from any to any port = 3162 keep state label "DemonwarePortMapping" rtable 0 -> 192.168.1.49 port 3074
```

Here is a pastebin dump of the packet capture, listening on 2189:

https://pastebin.com/24hkmCcJ

Let me know if you want the .cap file, and how you would prefer I deliver it.

Since it seems the redirected port jumps around while the game client (re)tries to get a upnp session, I'm not sure how to listen to traffic on that port without capturing all traffic from my brother's pc on the interface, which is what I have done. I'd be willing to share this directly, but not publicly.

Also, it seems that checking "Log Packets" does not put them in the syslog. After a cursory glance, I don't see that they're being logged at all. If I'm not looking in the right place, let me know.

If you need me to check anything else, I may not be able to until tomorrow. Hopefully this helps.

#33 - 05/18/2020 05:42 PM - Thomas BERNARD

Connor Ness wrote:

> If you need me to check anything else, I may not be able to until tomorrow. Hopefully this helps.

unfortunately it shows that everything is OK when the external port is mapped to the same internal port (3074 => 192.168.1.48:3074)
but it doesn't work for (3148 => 192.168.1.49:3074)

I don't know how to force pf to translate outgoing UDP packets from 192.168.1.49:3074 to src <public ip>:3148

my email address is available here : https://miniupnp.tuxfamily.org/

thank you.

#34 - 05/18/2020 06:03 PM - Connor Ness

Thank you very much, Thomas. I emailed the captures to you.

For what it's worth, I did have both PC's showing "Open" NAT types, and both were able to join each other's lobby, without upnp. I manually created port forwards and outbound mappings.

For outbound, I had:

192.168.1.48:3074 => WAN:13074
192.168.1.49:3074 => WAN:23074

For port forwards:

ANY:13074 => 192.168.1.48:3074
ANY:23074 => 192.168.1.49:3074

This worked, but my understanding is that this is what upnp should be able to achieve automatically. I'm imagining the process looks something like this:

1. PC1 requests upnp create outbound mapping and port forward for PC1:3074
2. upnp checks that a session is not currently alive for WAN:3074
3. there is no session, so create outbound mapping and port forward for WAN:3074 <=> PC1:3074, and we are done
4. PC2 requests upnp create outbound mapping and port forward for PC2:3074
5. upnp checks that a session is not currently alive for WAN:3074
6. there is a session, deny the request to PC2
7. PC2 requests upnp create outbound mapping and port forward for PC2:3076 (picked from a hat)
8. upnp checks that a session is not currently alive for WAN:3076
9. there is no session, so create outbound mapping and port forward for WAN:3076 <=> PC2:3076, and we are done

From what we're seeing, upnp is indeed creating these sessions, but the client is still unable to connect, so it retries until it decides no connection can be made. But with my manual port forwards and outbound mappings, it works as expected. Would it be worth setting those back up and comparing the entries?

#35 - 05/19/2020 09:38 AM - Jim Pingle

Thomas BERNARD wrote:

> unfortunately it shows that everything is OK when the external port is mapped to the same internal port (3074 => 192.168.1.48:3074)
> but it doesn't work for (3148 => 192.168.1.49:3074)
>
> I don't know how to force pf to translate outgoing UDP packets from 192.168.1.49:3074 to src <public ip>:3148

That's just a matter of using the right nat on rule.

Taking this specific inbound example:

```
rdr log quick on re0 inet proto udp from any to any port = 3148 keep state label "DemonwarePortMapping" rtable
 0 -> 192.168.1.49 port 3074
```

This is the equivalent outbound NAT example:

```
nat on re0 inet proto udp from 192.168.1.49 port 3074 to any -> (re0) port 3148
```

The (re0) is a pf macro which expands to the IP address on that interface. You can also explicitly specify the external IP address to use there.

EDIT: I removed some comments after this which were not relevant to the technical part of this discussion. If you want to discuss tangents/related topics, please move that discussion to a forum thread.

#36 - 05/19/2020 02:38 PM - Thomas BERNARD

thanks, so

```
nat on re0 inet proto udp from 192.168.1.49 port 3074 to any -> (re0) port 3148
```

is the additional pf rule that need to be created for outbound traffic when a port mapping (3148 => 192.168.1.49:3074 UDP) is created.

#37 - 05/19/2020 02:57 PM - Jim Pingle

Thomas BERNARD wrote:

> thanks, so
> [...]
> is the additional pf rule that need to be created for outbound traffic when a port mapping (3148 => 192.168.1.49:3074 UDP) is created.

Yes, that's the equivalent "outbound NAT" rule which would mirror the rdr rule. The only possible issue might be that it would be added to a "nat-anchor" instead of the "rdr-anchor". We have a couple NAT anchors (like "natearly") and I'm not sure if we can repeat a name in those to have "miniupnpd" exist in both nat-anchor and rdr-anchor tabs. I'd have to test that out. pf doesn't complain when I load it, but I didn't run a practical test. If the specific anchor names were config options that would be simple to work around either way.

#38 - 05/20/2020 07:29 PM - Thomas BERNARD

@jim
you can already have a look at what I've done :
https://github.com/miniupnp/miniupnp/pull/455

#39 - 05/22/2020 09:59 AM - Jim Pingle

Thomas BERNARD wrote:

> @jim
> you can already have a look at what I've done :
> https://github.com/miniupnp/miniupnp/pull/455

I'm not terribly familiar with pf code in C but if the result is what you show in your comments that's very promising. Though it shouldn't explicitly need the external IP address on the rule if you use the literal string '(re0)' for interface re0 pf will do the expected thing automatically and internally substitute the address.

Will this be an option behavior or only a compile-time choice? Seems like a good candidate for a command line parameter or config file knob.

#40 - 05/29/2020 05:38 PM - Thomas BERNARD

I don't know the equivalent of using '(re0)' with the ioctl() API. any pointer will be appreciated.

could you please test https://github.com/miniupnp/miniupnp/pull/455 ?

(my branch pf-nat-rules)

I'm not able to test myself, so I need testers or else I'll never validate theses changes.

#41 - 06/01/2020 02:22 PM - Jim Pingle

I don't know how that might be expressed in the ioctl/API, unfortunately. I've posed the question to some of our other developers and if I turn up anything, I'll pass it along.

I'll see about getting a version compiled with those changes for testing internally, thanks!

#42 - 06/01/2020 02:54 PM - Jim Pingle

According to one of our other developers, the (name) syntax is resolved by pfctl so it isn't in the API. It uses ifa_load() which in turn calls getifaddrs() which appears to be similar to what you're doing already so there probably isn't anything different you need to do.

#43 - 06/01/2020 03:45 PM - Jim Pingle

- File miniupnpd-2.1.20190210,1.txz added

I don't have two identical consoles with identical online games to test, but just testing with a upnp client I see the extra NAT rules for UDP and they appear to be correct, though I see two rules instead of the one I'd expect, the labels are different:

```
miniupnpd rules/nat contents:
nat log quick on igb2 inet proto udp from 192.0.2.87 port = 62322 to any keep state label "NAT-PMP 62322 udp" rtable 0 -> 192.xxx.xxx.111 port 62322
nat log quick on igb2 inet proto udp from 192.0.2.87 port = 62322 to any keep state label "192.0.2.87:62322" rtable 0 -> 192.xxx.xxx.111 port 62322
rdr log quick on igb2 inet proto tcp from any to any port = 62322 keep state label "192.0.2.87:62322" rtable 0 -> 192.0.2.87 port 62322
rdr log quick on igb2 inet proto udp from any to any port = 62322 keep state label "192.0.2.87:62322" rtable 0 -> 192.0.2.87 port 62322
pass in log quick on igb2 inet proto tcp from any to 192.0.2.87 port = 62322 flags S/SA keep state label "192.0.2.87:62322" rtable 0
pass in log quick on igb2 inet proto udp from any to 192.0.2.87 port = 62322 flags S/SA keep state label "192.0.2.87:62322" rtable 0
```

The client opened both a TCP and UDP forward for the same port, and as expected only the UDP one was reflected in the outbound NAT rule. Not sure where the second one came from but since it's labeled NAT-PMP it's different from all the others.

I am attaching a version of the miniupnpd pkg for pfSense 2.5.0 snapshots (must be on the latest available snapshots to use it). This code is not in snapshots, it must be installed manually. Updating to a new snapshot may replace this with the stock version, so be careful when updating.

If anyone else wants to test:

1. Download that file and copy it to the firewall (scp, fetch, etc)
2. Install it with this command, run from the directory with the file: pkg add -f miniupnpd-2.1.20190210,1.txz
3. From the GUI, save on the miniupnpd settings to restart it properly
4. Test.

To back it out if it doesn't work:

1. pkg delete -fy miniupnpd
2. pkg install -y miniupnpd

#44 - 06/01/2020 08:43 PM - Marc J

I disabled IPv6 from the WAN interface as I don't use it anyways.

Now I get this in the logs:

Seems possibly related to: https://redmine.pfsense.org/issues/10398 ?
I added the ext_ip to the "Override WAN address" without any luck here either.

```
@Jun 2 06:33:11    miniupnpd    26938    no HTTP IPv6 address, disabling IPv6
Jun 2 06:33:11    miniupnpd    26938    Listening for NAT-PMP/PCP traffic on port 5351
Jun 2 06:33:11    miniupnpd    26938    PCPSendUnsolicitedAnnounce() IPv6 sendto(): Bad file descriptor
Jun 2 06:40:05    miniupnpd    26938    ioctl(s, SIOCGIFADDR, ...): Can't assign requested address
Jun 2 06:40:05    miniupnpd    26938    ioctl(s, SIOCGIFADDR, ...): Can't assign requested address
Jun 2 06:40:05    miniupnpd    26938    Failed to get IP for interface pppoe0
Jun 2 06:40:05    miniupnpd    26938    SendNATPMPPublicAddressChangeNotification: cannot get public IP address, stopping
Jun 2 06:40:05    miniupnpd    26938    PCPSendUnsolicitedAnnounce() sendto(): No route to host
Jun 2 06:40:05    miniupnpd    26938    PCPSendUnsolicitedAnnounce() IPv6 sendto(): Bad file descriptor
Jun 2 06:40:11    miniupnpd    26938    SendNATPMPPublicAddressChangeNotification: sendto(s_udp=10, port=5351): No route to host
Jun 2 06:40:11    miniupnpd    26938    PCPSendUnsolicitedAnnounce() sendto(): No route to host
Jun 2 06:40:11    miniupnpd    26938    PCPSendUnsolicitedAnnounce() IPv6 sendto(): Bad file descriptor@
```

Thanks!

#45 - 06/03/2020 08:59 AM - Jim Pingle

I started a forum thread for people to share experiences testing this:
https://forum.netgate.com/topic/154153/test-request-upnp-fix-for-multiple-consoles-playing-the-same-game-static-port-outbound-nat

Let's keep the discussion there and only put information on this issue which is strictly relevant to the new changes.

#46 - 06/06/2020 01:36 PM - Thomas BERNARD

please test with miniupnpd-2.2.0-RC1.tar.gz
released on https://miniupnp.tuxfamily.org/files/

#47 - 06/06/2020 04:24 PM - Marc 05

Thomas BERNARD wrote:

> please test with miniupnpd-2.2.0-RC1.tar.gz
> released on https://miniupnp.tuxfamily.org/files/

I take it I have to wait for Jim to make a patched version for us to use in pfSense 2.5.

#48 - 06/10/2020 01:28 PM - Jim Pingle

We have added the 2.2.0-RC1 version of miniupnpd to the repository for pfSense 2.5.0 and so it should be included in snapshots shortly for additional (and easier) testing.

#49 - 06/10/2020 01:29 PM - Jim Pingle

- Status changed from New to Feedback

- Assignee set to Jim Pingle

- Target version set to 2.5.0

#50 - 06/11/2020 08:50 AM - Jim Pingle

The latest 2.5.0 snapshot now contains miniupnpd-2.2.0.r1,1 for testing

#51 - 09/16/2020 10:31 AM - Mike Smith

I believe pf is only capable of symmetric NAT. I know pfSense pf is different from FreeBSD pf but I'm curious about this FreeBSD pf patch from 2017 that was intended to implement full cone NAT into pf. The patch was never implemented so I'm wondering without the patch it's potentially not allowing miniupnpd to completely do it's job and instead is having to deal with symmetric NAT only.

https://reviews.freebsd.org/D11137

Interesting read on the different kinds of NAT's dealing with gaming:

http://badmodems.com/Forum/viewtopic.php?t=21

#52 - 01/09/2021 05:32 PM - Kris Phillips

Based on Feedback from testers on the forums, they are stating this is not fixed currently.

https://forum.netgate.com/topic/154153/test-request-upnp-fix-for-multiple-consoles-playing-the-same-game-static-port-outbound-nat/67?_=1610234284323&lang=en-US

#53 - 01/29/2021 09:25 PM - Polar Nerd

I can confirm that this is still a problem in 2.5.0.a.20210129.1122.
I upgraded a school system today from 2.3.x to 2.4.5-p1. Multiple game consoles were able to play prior to the upgrade.
After the upgrade, uPnP only provided one game console with a reservation, and the rest were strict NAT.
Based on this page, I upgraded to the latest snapshot 2.5.0.a.20210129.1122 and it still doesn't work.
I reinstalled 2.3.5.p2 and restored the configuration and multiple game consoles worked again.
I hope this is helpful.

#54 - 02/02/2021 11:18 AM - Renato Botelho

- Status changed from Feedback to New

#55 - 02/03/2021 02:32 PM - Renato Botelho

I just updated net/miniupnpd to 2.2.1 so it would be nice to get it tested again after that

#56 - 02/04/2021 09:11 AM - Renato Botelho

- Status changed from New to Feedback

Keith contacted me and said it will be tested during the weekend. Leave it in feedback state until hear about results

#57 - 02/09/2021 08:23 AM - YP Lo

I think other than adding the static NAT port entry (which is only for the single port requested by the console for external access with static NAT), it may also be useful to have an option that also automatically adds full static-port mapping entry added to pf via miniupnpd which ensures that any other dynamic ports used by the console will be also be statically mapped instead of being randomised by NAT. This is especially the case with Nintendo switch, which without static-port map will result in NAT Type D and can be resolved by doing static port map which changes it into NAT Type B [https://www.reddit.com/r/splatoon/comments/6rtgmg/nat_types_and_connection_problems_explained/] and also topic [https://forum.netgate.com/topic/112631/nintendo-switch-needs-static-port-on-its-outbound-nat/35].

The corresponding pf rule should be something like...

> nat on (wan-if) inet from (lan-ip) to any -> (wan-ip) static-port

The second "problem" I noticed is that uPnP mapped ports have its source address rewritten by NAT, while manual port-forwarded ports is a pure redirect. Is it possible to have miniuPnP add the port-forwarding entry without NAT? It is possible that some consoles require the WAN source address and doesn't work well with the NATed internal gateway IP address (which I presume is automatically added by 'Automatic outbound NAT rule generation' NAT mode configuration)?

#58 - 02/09/2021 08:34 AM - Marc 05

YP Lo wrote:

> Is it possible to have miniuPnP add the port-forwarding entry without NAT?

Can you explain in more detail what source -> destination you're seeing now, and what you believe would work better?

#59 - 02/09/2021 09:05 AM - Jim Pingle

YP Lo wrote:

> I think other than adding the static NAT port entry (which is only for the single port requested by the console for external access with static NAT), it may also be useful to have an option that also automatically adds full static-port mapping entry added to pf via miniupnpd which ensures that any other dynamic ports used by the console will be also be statically mapped instead of being randomised by NAT. This is especially the case with Nintendo switch, which without static-port map will result in NAT Type D and can be resolved by doing static port map which changes it into NAT Type B [https://www.reddit.com/r/splatoon/comments/6rtgmg/nat_types_and_connection_problems_explained/] and also topic [https://forum.netgate.com/topic/112631/nintendo-switch-needs-static-port-on-its-outbound-nat/35].

That isn't possible. First, because the Switch doesn't request UPnP so there is nothing to trigger the setup, and second, adding static port for more than one internal host is going to break for the second console, so it's best to do that manually.

> The second "problem" I noticed is that uPnP mapped ports have its source address rewritten by NAT, while manual port-forwarded ports is a pure redirect. Is it possible to have miniuPnP add the port-forwarding entry without NAT? It is possible that some consoles require the WAN source address and doesn't work well with the NATed internal gateway IP address (which I presume is automatically added by 'Automatic outbound NAT rule generation' NAT mode configuration)?

That isn't correct. UPnP rules only affect connections on WAN, so the net result is exactly the desired output. It wouldn't NAT anything to an "internal" gateway unless your configuration is very broken. UPnP sets up a port forward on WAN and (now) an additional outbound NAT rule for new connections leaving WAN using the same port requested by UPnP.

Sounds like you may have a misconfiguration, post on the forum to discuss and figure it out.

#60 - 02/09/2021 10:38 AM - Polar Nerd

> I can confirm that this is still a problem in 2.5.0.a.20210129.1122.
> I upgraded a school system today from 2.3.x to 2.4.5-p1. Multiple game consoles were able to play prior to the upgrade.
> After the upgrade, uPnP only provided one game console with a reservation, and the rest were strict NAT.
> Based on this page, I upgraded to the latest snapshot 2.5.0.a.20210129.1122 and it still doesn't work.
> I reinstalled 2.3.5.p2 and restored the configuration and multiple game consoles worked again.
> I hope this is helpful.

Last night we repeated this experiment with the latest snapshot 2.5.0.a.20210204.2250

Again:
1. Made a backup of the current system running 2.3.5.p2 after confirming that multiple game consoles were operating in "open" firewall status
2. Upgraded to 2.5.0.a.20210204.2250 making no other changes to the configuration, and only one game console was able to operate in "open" status
3. Reinstalled 2.3.5.p2 and restored configuration, again multiple game consoles worked in "open" status
4. Just for kicks I inserted a Netgear Nighthawk R8000 and it also allowed the game consoles to all work in "open" status.

The configuration is a simple layer 2 Ethernet network with a pfSense machine (Intel i5 with an SSD and 8 gigs RAM) connected to a Comcast modem with a single WAN IP address.

We aren't making any configuration changes, and I confirmed that the UPnP configuration is the same on 2.5.0.a.20210204.2250. Are there any changes that we need to make?
We can keep trying this every week until it works. If there is anything I can do or provide that will help diagnose and fix this problem, please let me know. Thank you

#61 - 02/09/2021 12:17 PM - Renato Botelho

- Status changed from Feedback to In Progress

- Target version changed from 2.5.0 to CE-Next

There is clearly more to be done here. Move to 2.5next

Files

miniupnpd-2.1.20190210,1.txz	64.3 KB	06/01/2020	Jim Pingle