pfSense - Bug #3395

DHCPv6 client pass rules need to come before bogons

01/14/2014 08:39 PM - Chris Buechler

Status:	Resolved	**Start date:**	01/14/2014
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	DHCP (IPv6)	**Estimated time:**	0.00 hour
Target version:	2.2.1		
Plus Target Version:		**Affected Version:**	2.1-IPv6
Release Notes:	Default	**Affected Architecture:**	

Description

8000::/1 is included in Cymru's v6 bogons list. That's sane, since it shouldn't be in the Internet routing table, but it breaks DHCPv6 clients as it blocks Advertise replies, which come from fe80 addresses. The best fix is probably moving the "allow dhcpv6 client" pass rules above the bogons block.

Associated revisions

Revision a60c6356 - 02/18/2014 01:00 PM - Renato Botelho

Move 'allow dhcpv6 client' rules above block bogonsv6 ones, it should fix #3395

Revision 8a4d1dbd - 02/18/2014 01:00 PM - Renato Botelho

Move 'allow dhcpv6 client' rules above block bogonsv6 ones, it should fix #3395

Revision 274a531a - 02/11/2015 04:59 PM - Chris Buechler

DHCPv6 client rules MUST come before bogons. Add a comment that hopefully sticks out so this stops getting broken. Ticket #3395

Revision 377b1faa - 02/11/2015 05:00 PM - Chris Buechler

DHCPv6 client rules MUST come before bogons. Add a comment that hopefully sticks out so this stops getting broken. Ticket #3395

History

#1 - 02/18/2014 01:00 PM - Renato Botelho

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset a60c6356ee22b081bdfe6b8a8dfd83865e6f2681.

#2 - 02/18/2014 01:00 PM - Renato Botelho

Applied in changeset 8a4d1dbd2a4d536201363a0f8d8a42fb6e057b33.

#3 - 03/06/2014 01:06 AM - Chris Buechler

- Status changed from Feedback to Resolved

works

#4 - 02/07/2015 10:26 PM - Paul K

I am experiencing this issue with v2.2. Rules look like this:

```
@51(1000001551) block drop in log quick on vmx0 from <bogons:3407> to any label "block bogon IPv4 networks fro
m WAN"
@52(1000001552) block drop in log quick on vmx0 from <bogonsv6:56131> to any label "block bogon IPv6 networks
 from WAN"
@53(1000001561) pass in quick on vmx0 inet6 proto udp from fe80::/10 port = dhcpv6-client to fe80::/10 port =
 dhcpv6-client keep state label "allow dhcpv6 client in WAN"
@54(1000001562) pass in quick on vmx0 proto udp from any port = dhcpv6-server to any port = dhcpv6-client keep
 state label "allow dhcpv6 client in WAN"
@55(1000001563) pass out quick on vmx0 proto udp from any port = dhcpv6-client to any port = dhcpv6-server kee
p state label "allow dhcpv6 client out WAN"
```

as you can see bogon rules are placed before dhcpv6 rules.

It seems like the fix for this bug was undone with commit 59c0272ec779cb917e5e1cabe779cc03bea7be47

#5 - 02/08/2015 02:38 AM - Kill Bill

Yes, this yet again got broken.

#6 - 02/11/2015 05:00 PM - Chris Buechler

- Status changed from Resolved to Feedback

- Target version changed from 2.1.1 to 2.2.1

Indeed. Fixed again, and added a comment that will hopefully prevent this from ever getting broken again.

#7 - 02/16/2015 03:46 PM - Paul K

Tested the patch on v2.2. Rules are now appearing in the correct order and DHCPv6 messages are not getting blocked.

```
@51(1000000561) pass in quick on vmx0 inet6 proto udp from fe80::/10 port = dhcpv6-client to fe80::/10 port =
 dhcpv6-client keep state label "allow dhcpv6 client in WAN"
@52(1000000562) pass in quick on vmx0 proto udp from any port = dhcpv6-server to any port = dhcpv6-client keep
 state label "allow dhcpv6 client in WAN"
@53(1000000563) pass out quick on vmx0 proto udp from any port = dhcpv6-client to any port = dhcpv6-server kee
p state label "allow dhcpv6 client out WAN"
@54(1000001561) block drop in log quick on vmx0 from <bogons:3407> to any label "block bogon IPv4 networks fro
m WAN"
@55(1000001562) block drop in log quick on vmx0 from <bogonsv6:56131> to any label "block bogon IPv6 networks
 from WAN
```

Thanks for fixing this again Chris.

#8 - 02/17/2015 11:24 PM - Chris Buechler

- Status changed from Feedback to Resolved

thanks for confirming.

#9 - 05/01/2016 02:59 PM - John Hood

This issue seems to have reappeared, though the separation of the rules involves suggests the exact cause might be different:

```
@62(11000) block drop in log quick on em1 from <bogonsv6:68342> to any label "block bogon IPv6 networks from L
AN"
  [ Skip steps: d=75 p=73 sp=73 da=73 dp=73 ]
  [ queue: qname= qid=0 pqname= pqid=0 ]
```

```
@76(1000002651) pass quick on em1 inet6 proto udp from fe80::/10 to fe80::/10 port = dhcpv6-client keep state
label "allow access to DHCPv6 server"
  [ Skip steps: i=82 d=80 f=82 p=82 sa=79 sp=81 dp=78 ]
  [ queue: qname= qid=0 pqname= pqid=0 ]
@77(1000002652) pass quick on em1 inet6 proto udp from fe80::/10 to ff02::/16 port = dhcpv6-client keep state
label "allow access to DHCPv6 server"
  [ Skip steps: i=82 d=80 f=82 p=82 sa=79 sp=81 da=79 ]
  [ queue: qname= qid=0 pqname= pqid=0 ]
@78(1000002653) pass quick on em1 inet6 proto udp from fe80::/10 to ff02::/16 port = dhcpv6-server keep state
label "allow access to DHCPv6 server"
  [ Skip steps: i=82 d=80 f=82 p=82 sp=81 dp=80 ]
  [ queue: qname= qid=0 pqname= pqid=0 ]
@79(1000002654) pass quick on em1 inet6 proto udp from ff02::/16 to fe80::/10 port = dhcpv6-server keep state
label "allow access to DHCPv6 server"
  [ Skip steps: i=82 f=82 p=82 sp=81 ]
  [ queue: qname= qid=0 pqname= pqid=0 ]
@80(1000002655) pass in quick on em1 inet6 proto udp from fe80::/10 to 2001:470:8bf0:1::1 port = dhcpv6-client
 keep state label "allow access to DHCPv6 server"
  [ Skip steps: i=82 f=82 p=82 ]
  [ queue: qname= qid=0 pqname= pqid=0 ]
@81(1000002656) pass out quick on em1 inet6 proto udp from 2001:470:8bf0:1::1 port = dhcpv6-server to fe80::/1
0 keep state label "allow access to DHCPv6 server"
  [ Skip steps: dp=90 ]
  [ queue: qname= qid=0 pqname= pqid=0 ]
```

This occurs on a system with DHCPv6 and "Block bogon networks" enabled on LAN0. Disabling bogons for the LAN interface causes DHCP6 to start working again.

I spent a while debugging this, at least I'm glad to know it's a well known problem :)

#10 - 05/01/2016 03:01 PM - John Hood

Oh, yes: 2.3-RELEASE amd64, originally installed with 2.2.1 or so and upgraded, and finally deployed after the upgrade.

#11 - 05/01/2016 04:30 PM - Chris Buechler

John Hood wrote:

> This issue seems to have reappeared

No, this was DHCPv6 client, you're referring to server. Unrelated. There is a separate ticket for bogons and DHCPv4 which is the same as this effectively. There's no reason to block bogon sources on your LAN in most all cases, that's for Internet connections.