strongSwan - Issue #2282

StrongSwan colliding with other processes accessing iptables

16.03.2017 00:42 - Olaf Martens

Status:	Closed		
Priority:	Normal		
Assignee:	Noel Kuntze		
Category:	configuration		
Affected version:	5.2.2	**Resolution:**	No feedback

Description

When I attempt to open a VPN connection to my server, the tunnel is brought up seemingly as usual, but occasionally may fail to open up correctly. In that event NetworkManager signals that the tunnel had been brought up, but no connection is possible.

A bit of poking around on my server had me dig up some interesting coincidences, though: Since I'm periodically running two scripts that are managing two blacklists (Spamhaus DROP/EDROP and the Fullbogon blacklist), these scripts are making extensive use of iptables, because these lists tend to be very long. However, since iptables obtains an exclusive lock on the IP tables and ipsec also uses iptables to establish its rules, the two may interfere with one another, thereby causing iptables to fail installing or deleting rules. The DROP and Bogon scripts use the -w option when invoking iptables so the program waits for the xtables lock is released, but this is not the case with StrongSwan. This after all is what is causing the VPN tunnel to not be properly opened and so connection attempts to fail: Due to critical rules not being installed, the server simply doesn't know how to properly handle the packets coming in via the VPN tunnel so nothing is returned.

I have done some tinkering and added the -w option to any call of iptables in the _updown script, but when I attempt to open the VPN tunnel after these modifications, the attempt times out.

To mitigate this problem, there are two things that need to be done:
1. Add the -w option to any call of iptables and ip6tables, causing iptables to wait on the xtables lock if another process has locked it. Since this option normally doesn't cause any overhead and also doesn't interfere with its normal operation, adding it doesn't hurt.
2. Send status messages from the remote end to the StrongSwan plugin so that NetworkManager knows that the remote end is still alive as long as the tunnel isn't completely set up. This helps avoid timeouts in case another process is using iptables concurrently with StrongSwan and allows for establishing the tunnel even though the IP tables are really busy - however, the process could take up quite some time.

History

#1 - 16.03.2017 01:04 - Noel Kuntze

Olaf Martens wrote:

> When I attempt to open a VPN connection to my server, the tunnel is brought up seemingly as usual, but occasionally may fail to open up correctly. In that event NetworkManager signals that the tunnel had been brought up, but no connection is possible.
>
> A bit of poking around on my server had me dig up some interesting coincidences, though: Since I'm periodically running two scripts that are managing two blacklists (Spamhaus DROP/EDROP and the Fullbogon blacklist), these scripts are making extensive use of iptables, because these lists tend to be very long.

That's absurdly inefficient. Use ipsets instead. Doing that prevents this problem from ever occuring, makes the loading of the blacklist more efficient and allows you to swap the sets atomically. Take a look at what I did with the blocklist from blocklist.de.
This is the best solution to this problem.

> However, since iptables obtains an exclusive lock on the IP tables and ipsec also uses iptables to establish its rules, the two may interfere with one another, thereby causing iptables to fail installing or deleting rules. The DROP and Bogon scripts use the -w option when invoking iptables so the program waits for the xtables lock is released, but this is not the case with StrongSwan. This after all is what is causing the VPN tunnel to not be properly opened and so connection attempts to fail: Due to critical rules not being installed, the server simply doesn't know how to properly handle the packets coming in via the VPN tunnel so nothing is returned.

ipsec itself has nothing to do with iptables. Your problem is likely with either the native modules that need to use iptables to insert rules or with the updown script.
You can change the latter to use -w.

> I have done some tinkering and added the -w option to any call of iptables in the _updown script, but when I attempt to open the VPN tunnel after these modifications, the attempt times out.

What exactly times out? The connection (packets aren't received or responded to by the remote peer) or the call to iptables hangs? Or does this have to do with networkmanager?
Logs, please in either case.

> To mitigate this problem, there are two things that need to be done:
> 1. Add the -w option to any call of iptables and ip6tables, causing iptables to wait on the xtables lock if another process has locked it. Since this option normally doesn't cause any overhead and also doesn't interfere with its normal operation, adding it doesn't hurt.
> 2. Send status messages from the remote end to the StrongSwan plugin so that NetworkManager knows that the remote end is still alive as long as the tunnel isn't completely set up. This helps avoid timeouts in case another process is using iptables concurrently with StrongSwan and allows for establishing the tunnel even though the IP tables are really busy - however, the process could take up quite some time.

You're talking about networkmanager-strongswan and not about the "normal" strongswan?

#2 - 11.04.2017 08:43 - Olaf Martens

I followed your suggestion of ipset and modified the scripts accordingly. This should avert any future problems of this sort if the bad IP lists are updated now.

#3 - 11.04.2017 09:49 - Noel Kuntze

Great. Could you please answer the questions I asked, please? That would be very helpful in categorizing this problem.

#4 - 21.05.2019 11:00 - Tobias Brunner

- Category set to configuration

- Status changed from New to Closed

- Assignee set to Noel Kuntze

- Resolution set to No feedback