pfSense - Bug #11699

OpenVPN does not clean up parsed ``Cisco-AVPair`` rules on non-graceful disconnect

03/18/2021 09:28 AM - Viktor Gurov

Status:	Closed	**Start date:**	03/18/2021
Priority:	Normal	**Due date:**	
Assignee:	Viktor Gurov	**% Done:**	0%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.5.2		
Plus Target Version:	21.05	**Affected Version:**	
Release Notes:	Default	**Affected Architecture:**	

Description

There is a difference between a graceful and not graceful disconnect. We tested it last night where I just turn off my WiFi adapter, then disconnected from VPN when logged in as TEST1 (with TEST1 related Cisco-AVPair ACLs). If I turned my WiFi adapter on and log in as my account with IT access, I get TEST1 access. However, if I disconnect my account, then log in as TEST1, click the disconnect, and log back into VPN using my account again, it appears to work.

It definitely seems like the VPN server hangs on to the account that didn't "gracefully" disconnect.

Associated revisions

Revision 58307d6f - 05/12/2021 07:13 AM - Viktor Gurov

Set default OpenVPN inactive timeout to 300. Issue #11699

Revision 9569d863 - 06/11/2021 10:53 AM - Viktor Gurov

OpenVPN Wizard: Set inactive_seconds = 300 by default.

Follow up with fix for ticket #11699 and also enable it on server
tunnels created using wizard

History

#1 - 03/18/2021 11:39 AM - Jim Pingle

According to the OpenVPN docs and other posts I see, the disconnect script should be run even on ping timeout / unclean disconnects, so perhaps there is something else amiss here.

There was one user who said it didn't work in some cases, but it's an old post and they didn't follow up if they were ever able to resolve it:
https://forums.openvpn.net/viewtopic.php?t=21869

#2 - 03/18/2021 12:07 PM - Viktor Gurov

Jim Pingle wrote:

> According to the OpenVPN docs and other posts I see, the disconnect script should be run even on ping timeout / unclean disconnects, so perhaps there is something else amiss here.
>
> There was one user who said it didn't work in some cases, but it's an old post and they didn't follow up if they were ever able to resolve it:
> https://forums.openvpn.net/viewtopic.php?t=21869

It works

After connecting:

```
# pfctl -a openvpn/ovpns1_raduser1_5558 -sr
pass in quick on ovpns1 inet proto udp from 3.3.3.3 to 7.7.7.7 port < 566 no state
pass in quick on ovpns1 inet proto udp from 3.3.3.3 to 7.7.7.7 port != 899 no state
```

Disconnect by timeout (inactive 100):

```
Mar 18 20:02:40 pf41 openvpn[76775]: TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.88.42:
1194
Mar 18 20:02:40 pf41 openvpn[76775]: UDPv4 link local (bound): [AF_INET]192.168.88.41:0
Mar 18 20:02:40 pf41 openvpn[76775]: UDPv4 link remote: [AF_INET]192.168.88.42:1194
Mar 18 20:03:40 pf41 openvpn[76775]: Inactivity timeout (--ping-restart), restarting
Mar 18 20:03:40 pf41 openvpn[76775]: SIGUSR1[soft,ping-restart] received, process restarting
Mar 18 20:03:42 pf41 openvpn[60506]: CA41client/192.168.88.5:5558 Inactivity timeout (--inactive), exiting
```

Result:

```
# pfctl -a openvpn/ovpns1_raduser1_5558 -sr
pfctl: DIOCGETRULES: Invalid argument
```

#3 - 03/19/2021 04:14 AM - Viktor Gurov

I think it is better to set the inactive timeout to the default value (like 300 seconds) for new instances
to cleanup ACL and DNS entries for non-graceful disconnected clients

#4 - 03/25/2021 01:17 AM - Viktor Gurov

Set default OpenVPN inactive timeout to 300:
https://gitlab.netgate.com/pfSense/pfSense/-/merge_requests/204

#5 - 03/29/2021 08:14 AM - Jim Pingle

- Status changed from New to Pull Request Review

- Target version set to CE-Next

- Affected Version deleted (2.5.0)

#6 - 05/11/2021 03:11 PM - Jim Pingle

- Plus Target Version set to 21.05

#7 - 05/12/2021 07:13 AM - Steve Beaver

- Status changed from Pull Request Review to Feedback

#8 - 05/12/2021 02:41 PM - Jim Pingle

- Subject changed from OpenVPN doesn't cleanup parsed Cisco-AVPair rules on non-graceful disconnect to OpenVPN does not clean up parsed ``Cisco-AVPair`` rules on non-graceful disconnect

Updating subject for release notes.

#9 - 05/27/2021 07:55 AM - Jim Pingle

- Target version changed from CE-Next to 2.5.2

#10 - 06/02/2021 01:26 PM - Jim Pingle

- Status changed from Feedback to Closed

#11 - 06/10/2021 04:17 AM - Viktor Gurov

This is not enabled for new servers created by the Remote Access Wizard.

fix:
https://gitlab.netgate.com/pfSense/pfSense/-/merge_requests/280

see also #11684#note-7

#12 - 06/16/2021 07:55 AM - Renato Botelho

- Assignee set to Viktor Gurov