pfSense - Bug #11328

OpenVPN Ciphers will not stick in 2.5

01/28/2021 03:56 PM - John Griffin

Status:	Resolved	**Start date:**	01/28/2021
Priority:	Very High	**Due date:**	
Assignee:	Steve Beaver	**% Done:**	100%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Plus Target Version:		**Affected Version:**	2.5.x
Release Notes:	Default	**Affected Architecture:**	

Description

So I upgraded my production home firwewall to 2.5 dev yesterday. None of the OpenVPN clients work after the upgrade despite connecting (i'll log a separate bug for that if I can work it out) but i'm attempting to create a new client to see whether that works.

I select the desired ciphers in the "Allowed Data Encryption Algorithms" (AES-256-GCM and AES-256-CBC). Hit save. Go back into the OpenVPN client config, and the ciphers have changed. It seems to like AES-256-GCM, AES-128-GCM and CHACHA20-POLY1305.

Associated revisions

Revision 2521eced - 02/02/2021 12:23 PM - Steve Beaver

Fixed #11328 by fixing jQuery and error when 'protocol' is undefined

History

#1 - 01/29/2021 08:22 AM - Jim Pingle

- Category changed from VPN (Multiple Types) to OpenVPN

- Status changed from New to Rejected

I can't reproduce this as stated. I was able to edit an existing client as well as create a new client, both times it respected the exact list I chose. I repeated the test with server entries and it worked as well.

#2 - 01/29/2021 04:49 PM - John Griffin

Here is video of it occurring. It seems a bit random, sometimes it works, sometimes you end up with a completely different set of ciphers.

https://youtu.be/eZtZxirQAFM
https://youtu.be/kUBZy0wKulU

Not sure of the protocol around here, as it's already been rejected should i submit another one? Will anyone ever read this :-)

#3 - 02/01/2021 07:39 AM - Jim Pingle

Those videos are private and cannot be viewed.

I tried again and can't replicate the problem here. Maybe write out a more complete procedure for replicating the problem, starting with a new/fresh tunnel. Also try different browsers, and make sure any script/ad blocking is disabled for the firewall URL.

#4 - 02/01/2021 07:05 PM - John Griffin

Sorry about the video's, they should be viewable now.

You are correct, I cannot replicate the issue in Firefox. I disabled every extension in chrome, then:

On a new blank clean build 2.5 instance I
a) created new CA
b) navigate to OpenVPN - Clients
c) Add
d) Fill in minimal information (remote server, username, password)
e) deselect AEs-128-GCM and CHACHA
f) added AES-256-CBC
g) hit save
go back in and the values will have changed

In the following video you can see that 2 out of 3 times the values were different when I went back in after saving

https://youtu.be/VMX661lJbcA

#5 - 02/02/2021 08:52 AM - Jim Pingle

- Status changed from Rejected to New

- Assignee set to Steve Beaver

- Priority changed from Normal to Very High

- Target version set to 2.5.0

OK, I can reproduce it that way, but only in Chrome. Watching the network panel as it makes the POST, for whatever reason Chrome is not sending the data_ciphers list in the POST. It happens to both clients and servers.

#6 - 02/02/2021 09:09 AM - Steve Beaver

- Status changed from New to In Progress

#7 - 02/02/2021 12:27 PM - Steve Beaver

- Status changed from In Progress to Feedback

- Assignee changed from Steve Beaver to John Griffin

#8 - 02/02/2021 12:30 PM - Steve Beaver

- % Done changed from 0 to 100

Applied in changeset 2521eced153b0c96bf6375787c607377e89639ed.

#9 - 02/02/2021 12:39 PM - Jim Pingle

- Assignee changed from John Griffin to Jim Pingle

#10 - 02/02/2021 12:46 PM - Jim Pingle

- Status changed from Feedback to Resolved

Works OK now in Chrome and FireFox. No JS errors on the list page or edit page.

#11 - 02/02/2021 12:47 PM - Jim Pingle

- Assignee changed from Jim Pingle to Steve Beaver