pfSense - Bug #2800

OpenVPN doesn't work properly with intermediate/chained CAs

02/07/2013 05:16 AM - Malte Stretz

Status:	Resolved	**Start date:**	02/07/2013
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	0%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.3.3		
Affected Version:	All	**Affected Architecture:**	

Description

There are two places where working with chained certificates is broken or at least weird. Background: OpenVPN always needs the whole CA chain in the --ca setting. It will also verify the client cert against the whole chain but that's not a pfSense problem.

So I've got this config: Created a Root CA with the pfSense Cert Manager. Created a VPN Intermediate CA with the Cert Manager. Created the OpenVPN server Cert within that CA and also the client certs.

In The OpenVPN settings I selected the Intermediate CA as the Peer Certificate Authority etc. I exported the client config with the OpenVPN Client Export Utility.

First issue: The OpenVPN Client Export Utility doesn't include the Root CA in the exported config thus the client will fail to connect. (Since I don't know if that package is an official pfSense package, this might be the wrong place to report this but this should be rather easy to fix.) It will fail with

> VERIFY ERROR: depth=1, error=unable to get local issuer certificate: /C=DE/ST=HH/L=HH/O=Example_GmbH/emailAddress=vpnmaster@example.net/CN=Example_VPN_CA__pfSense_

Second (more important) issue: Once the previous one is fixed manually, the server will also fail to verify the client cert with

> VERIFY ERROR: depth=2, error=self signed certificate in certificate chain: /C=DE/ST=HH/L=HH/O=Example_GmbH/emailAddress=hostmaster@example.net/CN=Example_Root_CA__pfSense_

If I set the Peer Certificate Authority to the Root CA, it looks like ti works (I have LDAP auth issues now but that's more than before).

This behaviour is at least weird/unintuitive and hard to debug. pfSense should either generate a proper chained cert if you select an Intermediate CA (preferred) or keep me from selecting one.

This is pfSense 2.0.2.

History

#1 - 01/04/2014 10:18 PM - Tim Lau

I am hit with the same bug.

Also, if you set the Peer Certificate Authority to the Root CA, 2 things happen:

1.
Certificate Depth in the Server tab needs to be adjusted.

2.
OpenVPN Client Export Utility stops working (Client Install Packages list becomes blank).

A potential workaround is to do the same for pfSense's OpenVPN server CA config as the solution to the first issue-
Append all the CA certificates in the chain to /var/etc/openvpn/server{x}.ca (root FS rw?)

Can anyone tell me the problem with this approach? (other than I shouldn't mess around with the FS directly).

#2 - 01/04/2014 10:32 PM - Tim Lau

After I posted the above, I have a new idea.

I just copied the Root CA certificate to the Intermediate CA's certificate in System: Certificate Authority Manager.

#3 - 01/08/2014 05:28 AM - Malte Stretz

You mean you essentially created a cert chain yourself in the Certificate Authority Manager and then it worked?

#4 - 07/26/2014 12:27 PM - Oliver Welter

Ran into the same issue today with version 2.1.4.
The hack to copy the full chain into the certmanager solves the problem but imho the correct behaviour should be to resolve the required certificates using the cert-manager and use the "extra-certs" option to provide the chain certificates.

#5 - 02/10/2015 11:39 AM - Bernd Zeimetz

Same broken behaviour in 2.2.

Adding the Root CA certificate to the Intermediate CA's certificate in System: Certificate Authority Manager still works as workaround.

#6 - 01/26/2016 10:32 PM - Taras Yermolenko

Hey guys,
Still having this issue on 2.2.6
Workaround is working

#7 - 07/12/2016 08:15 PM - Chris Buechler

- Status changed from New to Feedback

- Target version set to 2.4.0

- Affected Version changed from 2.0.x to All

Merged PR 2966 for 2.4 to address this.
https://github.com/pfsense/pfsense/pull/2966

If OpenVPN Client Export needs to be addressed still, that should have its own ticket under packages.

#8 - 11/03/2016 07:41 PM - Jim Thompson

- Assignee set to Jim Pingle

#9 - 11/04/2016 01:18 PM - Jim Pingle

- Status changed from Feedback to Resolved

This works fine in the base system and in the export package. I can make a CA, then make an intermediate CA, then make a server based on the intermediate, and a user based on the intermediate. Select the server cert and the server config has the full chain. Export the user cert and it has the full chain. Set the depth to 2 and the user connects fine. Looks good to me, closing the ticket.

#10 - 02/10/2017 10:22 AM - Jim Pingle

- Target version changed from 2.4.0 to 2.3.3

#11 - 04/25/2017 10:48 PM - Shane Fernando

Jim Pingle wrote:

> This works fine in the base system and in the export package. I can make a CA, then make an intermediate CA, then make a server based on the intermediate, and a user based on the intermediate. Select the server cert and the server config has the full chain. Export the user cert and it has the full chain. Set the depth to 2 and the user connects fine. Looks good to me, closing the ticket.

I can confirm this fixed the above issue with OpenVPN, but seems to introduce another problem if I use the Intermediate CA for LDAP+SSL. It breaks LDAP+SSL authentication, if the intermediate CA does not contain the full CA chain as per the workaround above.

#12 - 05/02/2017 01:47 PM - Diego Louzán

Hello guys, I have a very similar setup using v2.3.2 in AWS, I'm still hitting this issue, but in my case seems to be caused by line endings; I made an edit of my root CA's name, and this messed up the line endings of the exported cert (to CRLF). Meanwhile, the intermediate CA and client cert are stored in pfSense as LF. The effect is that when I export my OpenVPN configuration using the wizard, I end up with a file that mixes line endings for the different certs of the chain.