pfSense - Bug #8150

upgrade from 2.3* to 2.4* caused new self signed ssl cert to be selected for WebConfig

12/01/2017 02:34 AM - Oliver Schonrock

Status:	Not a Bug	**Start date:**	12/01/2017
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Affected Version:		**Affected Architecture:**	

Description

We recently upgraded several pfsense installs from 2.3.x to 2.4.y.

All these installs had properly signed SSL cert installed for the webconfigurator.

The upgrade generated a new self signed cert (not 100% sure this is accurate, maybe it was still there from earlier install), and then selected that self signed cert rather than the proper one.

because the domain uses HSTS and browsers won't allow you to make "security exceptions" for badly signed ssl certs in case of HSTS, we almost got a bit stuck. We solved it by ssh tunneling behind the upgraded install and accessing the webconfigurator from the "LAN" side.

History

#1 - 12/01/2017 09:18 AM - Jim Pingle

- Status changed from New to Not a Bug

The only way that will happen is if the certificate is invalid in some way. Missing entirely, incorrect reference, or missing the certificate or private key portions. See source:src/etc/inc/system.inc#L1326 - there isn't any way for that to happen during the upgrade that I can see, however. You can look through diffs between the configurations in the config history to see what changed.

Please start a thread on the forum, mailing list, or pfSense subreddit and discuss the problem a bit more in-depth there. If a specific bug can be identified, we can reopen this or start a new issue.

#2 - 12/01/2017 10:01 AM - Oliver Schonrock

Been using pfSense for 10years. Thanks to the team for all their efforts.

For what it's worth, here is the config history of the box which switched the cert.

```
11/30/17 20:46:17     17.3     67 KiB     admin@sanitised: /system_advanced_admin.php made unknown change
    11/30/17 20:41:03     17.3     67 KiB     (system): Generated new self-signed HTTPS certificate (5a206cdf2
b43d)
    11/30/17 20:40:51     17.3     62 KiB     (system): Upgraded config version level from 15.8 to 17.3
```

the top (most recent) line is me changing it back to the original proper cert after tunnelling into LAN. That cert works perfectly both before and after upgrade, so was "not broken" as far as I can see.

The other 2 lines are pfsense 2.4 coming up for first time and chosing to make a new self signed cert.

The carp peer of the box above didn't generate a self signed upon upgrade. This is it's first boot:

```
11/30/17 21:04:04     17.3     64 KiB     (system): Overwrote previous installation of iftop.
        11/30/17 21:04:03     17.3     64 KiB     (system): Intermediate config write during package removal f
or iftop.
```

```
        11/30/17 21:03:47     17.3     64 KiB     (system): Upgraded config version level from 15.8 to 17.3
```

Just trying to be helpful and record these things somewhere useful. If you want to close it as "not a bug", that's fine with me, since I am never going to do that specific upgrade again.

#3 - 01/09/2018 01:57 PM - Oliver Schonrock

Please reopen this bug, because I have managed to reproduce it with more detail.

While replacing the SSLs on this same CARP pair due to the Chrome trust issue:
https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

The same problem occurred. This is what I think is happening:

1. I upgrade the SSLs on the CARP master (add new cert, add new intermediate cert, switch webconfigurator to use new cert). Test => OK. Remove old cert and int-cert.

2. Switch to the CARP slave. because the "Certificate Authorities, Certificates, and Certificate Revocation Lists" option is ticked under "SystemHigh Availability Sync", the new cert, int-cert and webconfigurator "use new cert" options have already been synched by CARP

3. But the browser still reports the old cert, because nginx hasn't restarted yet (this normally happens when you switch the "webconfigurator use new cert" option under advanced settings)

4. So log into CARP slave on ssh console and use "restart webconfigurator" option (no option to do this from GUI I think).

5. BANG. pfSense generates a new self-signed cert and causes the abovementioned problems connecting to the GUI because this domain has HSTS enabled on it.

So I suspect this was never to do with upgrading to new version of pfSense, but to do with CARP sync of certs / "webconfigurator use cert" option.

I have turned off the "Certificate Authorities, Certificates, and Certificate Revocation Lists" option now to prevent this happening again, but really that's just a workaround. That option is not "safe" to use for a CARP pair in the current state.

Hope that helps.

#4 - 01/09/2018 02:26 PM - Jim Pingle

It's still not a bug. You didn't update the certificate on the secondary properly. The two units share a certificate store when set to synchronize, you can't select certificate on the secondary that doesn't exist on the primary, or naturally it will fail, and continue to fail since the "new" certificates will be overwritten every time the primary synchronizes the settings back.

1. Generate new cert on primary
2. Select new cert in GUI settings on primary (System > Advanced, Admin Access tab), Save
3. Go to secondary, the new cert from the primary should be synchronized there
4. Select the **exact same** cert in GUI settings on secondary (System > Advanced, Admin Access tab), Save

#5 - 01/09/2018 02:49 PM - Oliver Schonrock

Just to clarify...no certs are generated on the pfsense machines here...These are proper certs signed by a CA. Would you use self signed certs for production machines and put up with warnings? Anyway that wouldn't work if the domain uses HSTS, because the browser does not allow adding the sec exception.

I Agree that the slave did not get its cert upgraded properly, but the "webconfigurator should use cert" option was ALSO already synched on the slave...(but it was not actually using it).

I tried "saving it unchanged" ie with the new cert selected in the drop down, but that's a no-op and it doesn't restart the webserver etc.

I suspect that if I had had some random second cert available on the slave and changed to that, and then back to the new cert it would have worked. But really that what you want users to guess at?

I just don't think that option (sync certs) works safely at all, and is liable to lock you out, unless you operate the UI with a knowledge of how the code works underneath and bend over backwards to trick it into doing the right thing.

IMHO it's "extremely bad, bordering on unsafe, usability", if not a bug. I agree the use case is probably an edge case for basic consumer usage of pfSense (ie no CARP with self signed certs is probably 99%+ of usage), but for a production HA setup under HSTS, this "sync certs" option should be removed or fixed.

#6 - 01/09/2018 02:57 PM - Jim Pingle

I use ACME/Let's Encrypt certs where the certificate has SANs for both nodes + hostname(s) for the CARP VIP, and it works perfectly. The ACME package also has a mechanism to kick the secondary GUI to restart when the certificate is renewed. Even before that, however, I had no problems with self-signed certificates.

The GUI certificate selection under System > Advanced, Admin Access **does not synchronize**. If you load the page it's populated with the existing certificates but that doesn't mean it matches what is in config.xml. If you must do it manually, then you need to re-select the certificate there and then restart the GUI from the CLI after saving. It wouldn't be a no-op because the value in config.xml changed. Something else must not have been right when you did that.

If you would like to discuss the issue further, start a thread on the forum or reddit, but there is no bug here, additionally your scenario has nothing to do with the original problem as reported so it's not relevant to this issue.

#7 - 01/09/2018 03:26 PM - Oliver Schonrock

> I use ACME/Let's Encrypt certs where the certificate has SANs for both nodes + hostname(s) for the CARP VIP, and it works perfectly. The ACME package also has a mechanism to kick the secondary GUI to restart

different use case. a non-core package is doing all the work

> Even before that, however, I had no problems with self-signed certificates.

different use case. self signed certs don't need replacing in the same synchronised way and don't have the HSTS problem

> The GUI certificate selection under System > Advanced, Admin Access does not synchronize. If you load the page it's populated with the existing certificates but that doesn't mean it matches what is in config.xml.

Ahh so the GUI shows something which is not in config...very helpful..why does it not show "empty"?

> If you must do it manually

There is no other way to upgrade proper, long term, CA signed wildcard certs, is there?

> but there is no bug here,

It is clear you want that to be so. That's fine for me because I now know just not to use that "sync certs" option, because it is brittle/broken and the only way for it to work is to "trick" the GUI into doing the right thing for my use case with proper wildcard certs on HSTS which need upgrading.

What it probably is, is a regression, because before 2.4 this was not happening. I have been upgrading the certs on the same CARP pair for many years, and this was never an issue. It also never broke during pfSense upgrade before, and I have done dozens of upgrades over the years.

> has nothing to do with the original problem as reported so it's not relevant to this issue.

I can't prove it, but I would bet my little left finger that something changed in 2.4 which broke this (admittedly edge) use case, both during cert update and during pfSense 2.3=>2.4 upgrade. Or maybe... I never previously had that "cert sync" option turned on during upgrades before.

In any case, I will just keep that option turned off. It doesn't "work" reliably.

#8 - 01/09/2018 03:46 PM - Jim Pingle

Arguing won't help anyone. You won't convince anyone by acting that way, and there is nothing to "win". Clearly you are frustrated by the problem you encountered, but it is neither this problem nor a bug as stated. Discuss it in more detail on an appropriate platform (the forum, the pfSense subreddit, etc).

#9 - 01/09/2018 03:51 PM - Oliver Schonrock

Who's arguing? No me.

I was trying to point out that something was not working "quite right". Trying to help.

I have been using OSS for 15 years: writing it, contributing code, fixes, bug report etc.

I have never come across quite such a "shut door approach", before you had actually understood the problem. I still don't believe you have from your latest comments.

I am not frustrated. I think it's sad. Something has changed. This "approach" did not use to exist in pfSense. It's a far cry from the days when we retained Chris Buechler's consulting services to help us architect a secure production hosting environment using pfSense, 10 years ago. We still, in essence, use that architecture today. It's fantastic.

So why the change? New owner/shareholder?

Anyway, pfSense is not my core project or interest, just fringe, too many other irons in fires. So carry on.

Over and out.