pfSense - Feature #8641

Need way to disable HSTS and/or replace webConfigurator certificate from CLI

07/12/2018 05:22 PM - Adam Thompson

Status:	New	**Start date:**	07/12/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Web Interface	**Estimated time:**	0.00 hour
Target version:			

Description

On a 2.4.2-RELEASE firewall, which still sets the HSTS headers, I had a wildcard certificate installed, and it just expired. I forgot this firewall had that wildcard certificate installed or it would have been replaced long before expiry.
Now I'm stuck in a situation where I can't disable HSTS, and I can't replace the certificate because I can't log in because I haven't replaced the certificate because I can't log in... ad infinitum.
Catch-22.

My workaround was to use the PHP shell to set 'disablehsts' to true, i.e.
$config['system']['webgui']['disablehsts']=true;write_config();exit; and then restart webconfigurator from the console menu.
I don't think it's reasonable to expect the average admin to be able to figure that out - I only managed because I knew from dev work years ago what the "php shell" even **is**!

In theory, documenting this in a KB article or somewhere on the wiki - er, whatever's replacing the wiki, I mean - might be adequate, but given the likelihood of this being a problem while trying to regain internet access, I think it makes more sense as another menu item on the (yes, already crowded) console menu. Time for a submenu, maybe, for less-used / advanced functions?

History

#1 - 07/12/2018 05:23 PM - Adam Thompson

Yes, I'm aware of both #6650 and https://github.com/pfsense/pfsense/pull/3856, and I was able to find the Disable HSTS setting... once I was able to log back in! It's unfortunate, in many cases, although understandable, that HSTS is on by default.

Neither of those helps an admin who just made a mistake.

#2 - 07/12/2018 05:25 PM - Adam Thompson

And yes, I'd be happy to *also* write up a KB-style or doc-style page showing admins how to un-f*** themselves in this scenario, if you want.

#3 - 07/12/2018 05:42 PM - Jim Pingle

```
pfSsh.php playback generateguicert
```

#4 - 07/13/2018 07:32 AM - Adam Thompson

Thanks, Jim - that is much easier to type through a bad console connection! (Particularly since I just realized I've got several more systems in exactly the same situation. Oops.)

I'm still concerned that firewall administrators are likely to run into this problem at a time when they can't access documentation - specifically, the gateway device that has "just worked" for >1yr and suddenly needs attention because the connectivity is down... which means a limited ability to discover any way of fixing it that isn't baked in to what many might think of as the "emergency maintenance console".

The FR is to elevate one of these techniques to a discoverable menu item at the console (i.e. at 3am in the datacenter where you can't get a cell signal).

For the record, I'm very glad there exists ***a*** way to get oneself out of this corner with pfSense (unlike some other products).

Note for future readers (including myself 366 days from now):
Neither technique fully solves the problem by itself - Firefox, at least, refuses to switch from a "real" cert to a self-signed cert on a site with memorized

HSTS setting. You still have to clear FF's HSTS after regenerating the self-signed cert before it'll let you in. Make sure you know the password before telling FF to "Forget this site" or you'll create an entirely different problem.

#5 - 07/16/2018 08:38 AM - Jim Pingle

If you access the firewall by IP address instead of hostname, it should allow you to connect even with a bad cert IIRC. I don't have any that I can reproduce the issue against right now, but last time that happened accessing by name, accessing by IP address worked for me.

#6 - 07/16/2018 10:06 AM - Adam Thompson

While I now feel like a complete idiot, thank you for reminding me of the same advice I give to my own developers. Somehow troubleshooting certificates sent my brain down a different path where that didn't occur to me.

I've fixed all my affected instances now, so cannot test either, but I agree - I'm also 99% certain that using IP addresses would have worked.

This FR still isn't entirely stupid, but I agree that using IP addresses is an entirely acceptable alternative, in the absence of a (discoverable) way to manage this from the console.

Sorry for the noise :-(

#7 - 07/16/2018 10:21 AM - Jim Pingle

It's definitely a legitimate feature request. It makes sense to have a console menu entry that takes the GUI reset code from the "Set interface(s) IP address" code path and enhances it a bit. Right now it's buried and doesn't let you reset everything.

It could, for example, offer to:

- Regenerate a new self-signed GUI certificate
- Toggle HTTPS/HTTP
- Toggle HSTS
- Toggle OCSP Must Staple
- Toggle HTTP_REFERER Check
- Toggle DNS Rebinding Check
- Toggle GUI Redirect (80->current port)
- Toggle Anti-Lockout Rule