pfSense - Bug #6687

Secure email fails with private CA

08/09/2016 06:55 PM - Denny Page

Status:	Duplicate	**Start date:**	08/09/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Notifications	**Estimated time:**	0.00 hour
Target version:			
Plus Target Version:		**Affected Version:**	All
Release Notes:		**Affected Architecture:**	All

Description

If a private CA such as a self signed enterprise CA is in use, the CA is not recognized when establishing SMTP connections even though the CA certificate has been imported in System / Certificate Manager / CAs.

The reason for this is that the imported CA certificate is not stored in a location/manner available to OpenSSL. One solution (there may be others) to this issue is to append imported CA certificates to /usr/local/share/certs/ca-root-nss.crt.

History

#1 - 08/14/2016 05:35 AM - Kill Bill

Any attempts to do certificate validation here should be completely optional here (as in, a separate checkbox). **Way** too many mailservers have self-signed certificates or certificates that don't validate in one way or the other.

#2 - 08/14/2016 02:04 PM - Denny Page

The concept of an option to ignore certificate validation is completely unrelated to this issue.

#3 - 02/13/2017 07:03 PM - Ross Williams

I am interested in implementing a related feature that allows a "private CA" to be installed as a trusted root that is validated against when performing package updates. Appending to the ca-root-nss.crt file gets the job done, but is bad(tm) because that file belongs to an installed package. The better solution is to create a directory under /usr/local/etc/ssl called /usr/local/etc/ssl/crt and then configure OpenSSL to look there for additional certs.

I'm imagining that putting the OpenSSL environment variables that cause cURL to use that certs directory at the earliest point possible in the init process would also cause most other OpenSSL-based applications to also look for additional certs. Is this still an issue for you, Denny?

#4 - 02/13/2017 07:21 PM - Ross Williams

The root issue appears to be #4068.

#5 - 08/13/2019 02:55 PM - Jim Pingle

- Category set to Notifications

- Status changed from New to Duplicate

The root issue is definitely #4068, but an option was added to bypass this check in #9001 so this is a duplicate twice over.