pfSense - Feature #2904

Add checkbox or default option for "verify_identifier on;" on IPsec RSA VPNs

03/24/2013 06:33 PM - Jorge Albarenque

Status:	Resolved	**Start date:**	03/24/2013
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.1.1		
Release Notes:	Default		

Description

The ASN1DN field on the "peers_identifier" option within racoon.conf can be used to specify which certificate or set of certificates should be allowed to connect. Anyway, for this to take effect, there's an additional option required on the racoon.conf file:

verify_identifier on;

The default value for this is off. I guess this can be set to always on without harm, and increased security. If the ASN1DN values are left blank, they will be taken and verified from the certificates themselves. If you specify an ASN1DN manually, it will be used for verification.

In case I am missing something else that might break by adding this as a default option, a checkbox to enable it will be great.

Check my post about the topic and the racoon.conf man page for more info.

Thanks!

Associated revisions

Revision 6d0f5a63 - 02/28/2014 02:25 PM - Renato Botelho

Add an option to verify peers_identifier when it's ASN.1 distinguished name. It should fix #2904

History

#1 - 02/27/2014 01:01 PM - Doktor Notor

Guys, this is NOT a feature request, this is a major security issue! Can someone finally fix this?

https://forum.pfsense.org/index.php/topic,65002.0.html

#2 - 02/28/2014 02:30 PM - Renato Botelho

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset 6d0f5a635aed336e5d2b6208a07a564b79f8863d.

#3 - 02/28/2014 02:55 PM - Doktor Notor

Yay! Excellent, works just fine.

#4 - 02/28/2014 02:57 PM - Renato Botelho

- Status changed from Feedback to Resolved

#5 - 02/28/2014 02:57 PM - Renato Botelho

- Category set to IPsec

- Target version set to 2.1.1

- Affected Version set to 2.1