pfSense - Bug #7929

IPSec CA certificate name corrupt if multiple RDNs of the same type are in subject name

10/12/2017 01:43 AM - Daniel Sands

Status:	Resolved	**Start date:**	10/12/2017
Priority:	High	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Certificates	**Estimated time:**	0.00 hour
Target version:	2.4.2		
Affected Version:	2.3.4_1	**Affected Architecture:**	All

Description

When the CA certificate subject is converted to OSF style, but multiple RDN components of the same type are in the subject, the subject will be written out as something like:

/DC=Array/CN=MyCert/

This causes the IPSec server to dismiss the CA and fail to authenticate the client certificate.

The DC components might be DC=example,DC=com, in this case. In /etc/inc/vpn.inc, there is a foreach that adds the components one-by-one into this string. The loop needs to check whether the current component is an array or a value, and act appropriately for each case.

My quick and dirty local fix went as such:

```
                        if (!empty($ph1ent['caref'])) {
                                $ca = lookup_ca($ph1ent['caref']);
                                if ($ca) {
                                        $casubarr = cert_get_subject_array($ca['crt']);
                                        $casub = "";
                                        foreach ($casubarr as $casubfield) {
                                                if (empty($casub)) {
                                                        $casub = "/";
                                                }
                                                if (is_array($casubfield['v'])) {
                                                        foreach ($casubfield['v'] as $casubfieldco
mp) {
                                                                $casub .= "{$casubfield['a']}={$ca
subfieldcomp}/";
                                                        }
                                                }
                                                else
                                                {
                                                        $casub .= "{$casubfield['a']}={$casubfield
['v']}/";
                                                }
                                        }
                                }
                        }
```

Associated revisions

Revision 7e37da2e - 11/03/2017 10:27 AM - Jim Pingle

When crafting the CA subject for ipsec.conf, handle component values that are arrays. Fixes #7929

History

#1 - 10/27/2017 07:06 AM - Jim Pingle

- Category set to Certificates

- Assignee set to Jim Pingle

- Target version set to 2.4.2

#2 - 11/03/2017 10:40 AM - Jim Pingle

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset 7e37da2e9db8dd153e3b8ef2844beb9a9fe24a56.

#3 - 11/05/2017 01:15 AM - Constantine Kormashev

2.4.2 17-11-04 could not reproduce the issue
rightca for latest /DC=jimp/DC=pw/
rightca for 2.4.1 /DC=Array/
Auths works fine

#4 - 11/05/2017 08:04 AM - Jim Pingle

- Status changed from Feedback to Resolved