pfSense - Feature #9884

Add support for OpenVPN --x509-username-field

11/05/2019 05:20 AM - Florian Apolloner

Status:	Resolved	**Start date:**	11/05/2019
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.5.0		

Description

The openvpn shipped with pfsense has enable_x509_alt_username=no as compilation option. It would be great if that could turn on to enable reading the CN from different fields in the subject DN. This is helpful to be used together with " Strict User-CN Matching " to match the supplied username against a subject alt name or another field in the subject DN.

Associated revisions

Revision efe83ab9 - 11/21/2019 03:31 PM - Jim Pingle

Enable OpenVPN x509-alt-username build option. Fixes #9884

History

#1 - 11/05/2019 07:21 AM - Jim Pingle

- Tracker changed from Bug to Feature

- Subject changed from OpenVPN does not support --x509-username-field to Add support for OpenVPN --x509-username-field

- Category changed from VPN (Multiple Types) to OpenVPN

- Affected Version deleted (2.4.4-p3)

- Affected Architecture deleted (amd64)

This isn't a bug, but a missing feature. Even if it is enabled, it would still need GUI code to configure the behavior.

There is an option in the FreeBSD port to enable it, X509ALTUSERNAME=yes, so it could be enabled in source:tools/conf/pfPorts/make.conf without requiring any alterations to the port itself.

#2 - 11/05/2019 07:41 AM - Florian Apolloner

Sorry, I realized that it's not a bug immediately after clicking save, but I cannot edit anything :/

> Even if it is enabled, it would still need GUI code to configure the behavior.

One could enable it via "Custom options", so there is no real GUI need for it. Given that it is a rather special Option I'd be fine with doing that as a custom option.

#3 - 11/05/2019 07:47 AM - Jim Pingle

We currently force on username-as-common-name so I don't think you could override that behavior with this new option without some way to control which is used.

#4 - 11/05/2019 07:54 AM - Florian Apolloner

That is true, but it doesn't seem to affect "plugin /usr/local/lib/openvpn/plugins/openvpn-plugin-auth-script.so /usr/local/sbin/ovpn_auth_verify_async" (which pfsense also generates) as this script still has the actual common name from the cert (which --x509-username-field would affect) in addition to the user. If this common_name were overriden by the username then "Strict User-CN Matching" would always be true (it isn't, I checked which prompted me to try --x509-username-field). Or do I miss something else here?

#5 - 11/21/2019 03:32 PM - Jim Pingle

- Assignee set to Jim Pingle

- Target version set to 2.5.0

I'm not seeing any negative effects to enabling that build option, so it should be fine for testing.

#6 - 11/21/2019 03:40 PM - Jim Pingle

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset efe83ab95d64d8d364d8a210d709fa49a551e718.

#7 - 01/06/2020 03:10 PM - Jim Pingle

- Status changed from Feedback to Resolved

```
: pkg info openvpn | grep -i ALTUSER
    X509ALTUSERNAME: on
```

Also no apparent negative effects reported so far.