

pfSense - Feature #3377

OAuth2 authentication in captive portal

12/31/2013 04:56 AM - Thomas NOEL

Status:	New	Start date:	12/31/2013
Priority:	Normal	Due date:	
Assignee:	Jim Thompson	% Done:	0%
Category:	Captive Portal	Estimated time:	20.00 hours
Target version:	2.5.0		

Description

In Captive Portal we have native, ldap and radius authentication. Today, a lot of authentication systems provide OAuth2 backend. As CP authenticate users through web, it can be a OAuth2 client.

My idea is to add a new "OAuth2 Authentication" after "RADIUS Authentication" on CP configuration.

- RADIUS Authentication
 - Radius Protocol
 - PAP
 - CHAP_MD5
 - MSCHAPv1
 - MSCHAPv2
- OAuth2 Authentication
 - OAuth2 accepted providers
 - Amazon
 - BitLy
 - Box
 - Dailymotion
 - Dropbox
 - Facebook
 - Foursquare
 - GitHub
 - Google
 - Heroku
 - Instagram
 - LinkedIn
 - Microsoft
 - PayPal
 - RunKeeper
 - SoundCloud
 - Vkontakte
 - Yammer
 - Reddit
 - Local1
 - Local2

Local1, Local2, ... are local providers found in /usr/local/oauth2/local-providers/, for example.

Of course, there is other parameters (key/secret for each oauth2 provider). And we have to open HTTPS for all selected OAuth2 providers -- that is not very hard with "allowed hostnames".

I think that <https://github.com/Lusitanian/PHPoAuthLib> could be a good OAuth2 implementation to use. Add local providers is easy with this module.

Do you think such a feature is a good idea ? If there is no rebuttal, I can write a first proposal for a patch...

History

#1 - 12/31/2013 09:52 AM - Ermal Luçi

Sure go ahead.

#2 - 01/09/2014 04:42 AM - Thomas NOEL

Here is a proof of concept, for a OAuth2 captive portal authentication with Google accounts :

https://github.com/entrouvert/pfsense/tree/RELENG_2_1

The README.md file explains how to activate it.

Note : we have made changes on the RELENG_2_1 branch, because we can test them on pfSense 2.1 ISO. Is there a pfSense "master" ISO (future 2.2) somewhere ?

#3 - 01/10/2014 01:38 AM - Chris Buechler

there will be publicly-available 2.2 snapshots in the not too distant future. At this point, I think you might be ok running master code on a 2.1 install. If you gitsync to master, that may work fine, but I'd do that in a VM you can blow away and reinstall just in case.

https://doc.pfsense.org/index.php/Updating_pfSense_code_between_snapshots

#4 - 01/21/2015 11:28 AM - simon mitnick

Thomas NOEL wrote:

Here is a proof of concept, for a OAuth2 captive portal authentication with Google accounts :

https://github.com/entrouvert/pfsense/tree/RELENG_2_1

The README.md file explains how to activate it.

Note : we have made changes on the RELENG_2_1 branch, because we can test them on pfSense 2.1 ISO. Is there a pfSense "master" ISO (future 2.2) somewhere ?

Dear All,

I'm sorry if I have wrote in the wrong place...

I write for asking a support in order to include OAuth2 in pfSense CP. I don't catch the point how I can simulate on virtual environment the callback URI with private IP addresses?

Do you know some workaround for having (i.e <https://cpfsense:8001/index.php> as valid callback URI.

(pfsense= 192.100.xxx.xxx)

Error message by Google OAuth2 Login:

Invalid parameter value for redirect_uri: Non-public domains not allowed: <https://pfsense:8001/index.php>

I'm starting my project from https://github.com/entrouvert/pfsense/tree/RELENG_2_1 but I'm not able to test in virtualbox!

Any help is appreciate.

cheers

Simon

#5 - 05/24/2015 02:14 PM - bamidele Amire

Chris Buechler wrote:

there will be publicly-available 2.2 snapshots in the not too distant future. At this point, I think you might be ok running master code on a 2.1 install. If you gitsync to master, that may work fine, but I'd do that in a VM you can blow away and reinstall just in case.
https://doc.pfsense.org/index.php/Updating_pfSense_code_between_snapshots

Pls can I get a link to download an ISO that has the oauth option for authentication?

#6 - 08/15/2016 07:37 PM - Cleber Ronaldo

Thomas NOEL wrote:

In Captive Portal we have native, ldap and radius authentication. Today, a lot of authentication systems provide OAuth2 backend. As CP authenticate users through web, it can be a OAuth2 client.

My idea is to add a new "OAuth2 Authentication" after "RADIUS Authentication" on CP configuration.

[...]

Local1, Local2, ... are local providers found in /usr/local/oauth2/local-providers/, for example.

Of course, there is other parameters (key/secret for each oauth2 provider). And we have to open HTTPS for all selected OAuth2 providers -- that is not very hard with "allowed hostnames".

I think that <https://github.com/Lusitanian/PHPoAuthLib> could be a good OAuth2 implementation to use. Add local providers is easy with this module.

Do you think such a feature is a good idea ? If there is no rebuttal, I can write a first proposal for a patch...

News about this topic???

#7 - 08/23/2016 09:23 PM - Jim Thompson

- Assignee set to Jim Thompson

- Target version changed from Future to 2.4.0

Cleber Ronaldo wrote:

Thomas NOEL wrote:

In Captive Portal we have native, ldap and radius authentication. Today, a lot of authentication systems provide OAuth2 backend. As CP authenticate users through web, it can be a OAuth2 client.

My idea is to add a new "OAuth2 Authentication" after "RADIUS Authentication" on CP configuration.

[...]

Local1, Local2, ... are local providers found in /usr/local/oauth2/local-providers/, for example.

Of course, there are other parameters (key/secret for each oauth2 provider). And we have to open HTTPS for all selected OAuth2 providers -- that is not very hard with "allowed hostnames".

I think that <https://github.com/Lusitanian/PHPoAuthLib> could be a good OAuth2 implementation to use. Adding local providers is easy with this module.

Do you think such a feature is a good idea? If there is no rebuttal, I can write a first proposal for a patch...

News about this topic???

Looks straight-forward to add. Just ran across this.

#8 - 08/24/2016 05:27 PM - Kristian Junkov

Thomas NOEL wrote:

In Captive Portal we have native, ldap and radius authentication. Today, a lot of authentication systems provide OAuth2 backend. As CP authenticate users through web, it can be a OAuth2 client.

My idea is to add a new "OAuth2 Authentication" after "RADIUS Authentication" on CP configuration.

Is there any reason why it should only be limited to Captive Portal? I would love to use my Azure AD via OAuth2 for OpenVPN. I have been looking into a oauth2 perl module for freeradius (<https://github.com/jimdigriz/freeradius-oauth2-perl>) but being able to use oauth directly as a backend if pfSense would be even better.

Another thing, if OAuth is added as a backend userdb for pfsense, would it be possible to enable the freeradius server in pfsense to do the same? (Most network appliances only speak radius e.g. access points, managed switches etc.)

Really looking forward for any updates on this feature. Being able to utilize the cloud (user database) for pfsense would really be a quality of life improvement!

Best regards
Kristian

#9 - 08/24/2016 07:45 PM - Jim Thompson

Kristian Junkov wrote:

Thomas NOEL wrote:

In Captive Portal we have native, ldap and radius authentication. Today, a lot of authentication systems provide OAuth2 backend. As CP authenticate users through web, it can be a OAuth2 client.

My idea is to add a new "OAuth2 Authentication" after "RADIUS Authentication" on CP configuration.

Is there any reason why it should only be limited to Captive Portal? I would love to use my Azure AD via OAuth2 for OpenVPN. I have been looking into a oauth2 perl module for freeradius (<https://github.com/jimdigriz/freeradius-oauth2-perl>) but being able to use oauth directly as a backend if pfsense would be even better.

Another thing, if OAuth is added as a backend userdb for pfsense, would it be possible to enable the freeradius server in pfsense to do the same? (Most network appliances only speak radius e.g. access points, managed switches etc.)

Really looking forward for any updates on this feature. Being able to utilize the cloud (user database) for pfsense would really be a quality of life improvement!

Best regards
Kristian

My preference is to keep this limited to CP for now.

That said, your idea has merit, and I'd appreciate it if you opened a separate feature request for same.

#10 - 08/25/2016 12:51 PM - Kristian Junkov

My preference is to keep this limited to CP for now.

That said, your idea has merit, and I'd appreciate it if you opened a separate feature request for same.

Thanks! I have made a separate feature request here: <https://redmine.pfsense.org/issues/6742>

BR Kristian

#11 - 07/07/2017 03:29 PM - Jim Pingle

- Target version changed from 2.4.0 to 2.4.1

#12 - 10/12/2017 10:13 AM - Jim Pingle

- Target version changed from 2.4.1 to 2.4.2

#13 - 10/23/2017 12:18 PM - Jim Pingle

- Target version changed from 2.4.2 to 2.4.3

#14 - 12/05/2017 11:30 PM - Ponvannan Sankaran

is there further developments on the above feature radius with oauth backend to support google apps id it will be very nice feature i will give +1

#15 - 01/16/2018 02:08 PM - Jim Pingle

- Target version changed from 2.4.3 to 2.4.4

#16 - 08/14/2018 02:06 PM - Steve Beaver

- Target version changed from 2.4.4 to 48

#17 - 03/12/2019 10:54 AM - Jim Pingle

- Target version changed from 48 to 2.5.0