# Configuration pfSense

UAuth : Portail captif dans le Cloud

Entr'ouvert SCOP - http://www.entrouvert.com

#### Table des matières

1	Configuration d'un portail captif pfSense	1
2	Test d'authentification	5
Ce	document spécifie les étapes de configuration d'un portail captif pfSense pour son raccor	de-

ment à la plateforme U-Auth.

## 1 Configuration d'un portail captif pfSense

#### Dans le menu Services/Captive Portal

<b>Sense</b>	▶ System	▶ Interfaces	▶ Firewall	✓ Services	▶ VPN	<ul> <li>Status</li> </ul>	▶ Diag	nostics	▶ Gold	▶ Help		a pfSe	nse.entrouvert.lan
	Status: D	ashboard	I	Captive Ports DHCP Relay DHCP Server DHCPv6 Relay								2	
				DNS Forward	er								
	System Info	ormation		DNS Resolver		Inter	taces					크폰	
	Name	ptSens	e.entrouvert.lan	Dynamic DNS			(AN (P)	+	1000ba	sel <tull-du< td=""><td>olex&gt;</td><td></td><td></td></tull-du<>	olex>		
and the second second	Version	2.2.1-R built on	ELEASE (amd64) Fri Mar 13 08:16:	IGMP proxy			.,		10.0.2.1				
		FreeBS	D 10.1-RELEASE	Load Balance		<u></u> _	AN	+	1000ba	sel <full-du< td=""><td>olex&gt;</td><td></td><td></td></full-du<>	olex>		
and the second se		You are	e on the latest ve	NTP				_	10.42.0	.1			
and the second second	Platform	pfSens	e	PPPoE Server		Serv	ices Stati	IS					
	CPU Type	Intel(R)	Core(TM) i5-3230	SNMP @ 2.60		54	ruice		Descriptio		Statue		
and the second	Uptime 00 H	00 Hou	r 05 Minutes 19 S	UPnP & NAT-	MP	aning	er	Gateway	Monitorina	Daemon	Juurs	രര	
	Current	Wed Ma	ar 25 10:50:29 CE	Wake on LAN		canti	/enortal	Cantive Pr	vtal: teet	Decomon		00	
	date/time			_		dhan	a	DUCR Corr	vice.			00	
	DNS	127.0.0 91.121	.1 58.181			uncp	u	UTD stast	vice				
	server(s)	87.98.1	49.171			npu		NIF Clock	sync				
	Last config change	Tue Ma	r 24 17:32:25 CE	T 2015		unbo	una	Unbound L	JNS Kesoli	er			
	State table					Capt	ive Portal	Status					
	size	0% (66 Show s	/98000) states			IP ad	dress	MAG	address		Usernam	ie	
	MBUF Usa	ge 🚺	0/26584)										
	Load avera	age 0.10, 0.	22, 0.14										
	CPU usage	0%											
	Memory usage	23% of	989 MB										
	SWAP usa	ge 0% of 3	L024 MB										
https://10.42.0.1/s	Disk usane services_captiv	(ufs): reportal.php	37% of 992M										

ajouter une nouvelle zone :

<b>Sense</b>	▶ System	► Interfaces	▶ Firewall	▶ Services	► VPN	▶ Status	Diagnostics	▶ Gold	▶ Help	쓹 pfSense.e	ntrouvert.lan
	Service	s: Captive	portal: E	dit Zones	i					- 0 - C	
	Edit Captive	Portal Zones									
	Zone name	1	📏 edusp Zone name.	ot Can only contair	n letters, dig	jits, and under	scores (_).				
	Description	I	Nou may en	ter a description	here for yo	ur reference (	not parsed).				
			Continu	e							

Configurer la zone ainsi créée :

1. activer la zone :

Sense /	► System ► Interfaces	▶ Firewall ▶ Services	► VPN ► Status	Diagnostics Gold	▶ Help	ge pfSense.entrouvert.lan
	Captive portal(s) MAC Allo	wed IP addresses Allowed H	Hostnames Vouchers	File Manager		
		🖉 Enable captive porta	I			
	Interfaces	WAN A LAN V Select the interface(s) to e	enable for captive portal.			
	Maximum concurrent connections	per client IP This setting limits the numl many users can be logged the same time! Possible se connections.	address (0 = no limit) ber of concurrent connection in to the captive portal, bu tting allowed is: minimum 4	ons to the captive portal HTTP(S trather how many users can loa L connections per client IP addr	i) server. This does not set I the portal page or auther ess, with a total maximum	how ticate at of 100
	ldle timeout	minutes Clients will be disconnecte blank for no idle timeout.	d after this amount of inact	tivity. They may log in again im	mediately, though. Leave t	this field

2. configurer l'URL de redirection vers le page de connexion U-Auth :

<sup>oo</sup> Sense	► System ► Interfaces	Firewall    ▶ Services    ▶ VPN	e.entrouvert.lan
COUNCE	attempted access	If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.	
	Logout popup window	Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.	
	Pre-authentication redirect URL	https://u-auth.dev.entrouvert.org/pfsense-example Use this field to set\$PORTAL_REDIRURL\$ variable which can be accessed using your custom captive portal index.php page or error pages.	
	After authentication Redirection URL	Source a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.	
	Blocked MAC address redirect URL	S If you provide a URL here, MAC addresses set to be blocked will be redirect to that URL when attempt to access anything.	

- 3. configurer l'authentification Radius :
- protocole d'authentification : PAP
- adresse IP du serveur U-Auth : 176.31.146.80
- secret partagé : testing123

<b>Sense</b>	▶ System	► Interfaces	▶ Firewall	▶ Services	▶ VPN	▶ Status	<ul> <li>Diagnostics</li> </ul>	▶ Gold	▶ Help	; ga pfSense.e	ntrouvert.lan
	Authentic	ation	O No Au Local	thentication User Manager / Vo ② , US Authentication	ouchers Allow only user	s/groups with 'C	aptive portal login' privi	lege set			
			RADIUS I Primary	Protocol	PAP CHAP_MD5 MSCHAPv1 MSCHAPv2 n Source						
			Primary R	ADIUS server s Noter Enter	176.31.146 r the IP addres:	5.80 s of the RADIU	S server which users of	the captive p	ortal have to a	uthenticate against.	
			Port	N Leav	e this field blar	nk to use the de	fault port (1812).				
			Shared se	cret N Leav	testing123 e this field blar	nk to not use a l	ADIUS shared secret (	not recommer	ided).		

4. définir un nom local pour le portail captif :

<b>Sense</b>	<ul> <li>System</li> </ul>	► Interfaces	▶ Firewall	▶ Services	▶ VPN	▶ Status	<ul> <li>Diagnostics</li> </ul>	▶ Gold	▶ Help	묽 <mark>e</mark> pfSense	.entrouvert.lan
				ietf: ( cisco unfor	00-11-22-33-4 : 0011.2233.4 matted: 00112	4-55 455 22334455					
	HTTPS Io	gin	🗹 Enab If enabled A server na	e HTTPS login , the username a ume and certific:	.nd password ate must also	will be transm be specified	itted over an HTTPS below.	connection	to protect aga	ainst eavesdroppers.	
	HTTPS se	rver name	📏 pfser	se.example.o	org						
			This name certificate resolve this	will be used in t (otherwise, the o name in DNS a	the form acti lient browse and verify on	on for the HTT r will most like the client that	PS POST and should y display a security w the IP resolves to the	i match the arning). Mai correct inte	Common Nam e sure captive rface IP on pf	me (CN) in your re portal clients can fSense.	
	SSL Certif	icate	webConfi	gurator default (S	54f0a0b99b5	5d6) ▼					

5. desactiver le HTTPS Forwards



6. personnaliser la page d'authentification du portail captif en chargeant un fichier html contenant obligatoirement la variable \$PORTAL\_REDIRURL\$ :

<b>Sense</b>	<ul> <li>System</li> </ul>	Interfaces	▶ Firewall	Services	▶ VPN	▶ Status	<ul> <li>Diagnostics</li> </ul>	Gold	<ul> <li>Help</li> </ul>	he pfSens	se.entrouvert.lan
	Disable H	TTPS forwards	Disab If this option prevents connector redirected	ole HTTPS forway on is set, attempt ertificate errors f 1 to an HTTP (Po to the HTTPS to	rds s to connect rom being pr ort 80) site to ogin page.	to SSL/HTTP esented to the get forwarded	S (Port 443) sites will user even if HTTPS to the captive portal	l not be forwa logins are en I. If HTTPS lo	rded to the ca abled. Users n gins are enabl	ptive portal. This nust attempt a led, the user will be	
	Portal pag	e contents	G Chc View curre Download Restore de Upload an (POST to: value="\$P authentic: -form met -input -input -input -input -input -input -input -input -input -input	nose File No intpage current page fault portal page #TML/PHP file \$PORTAL_ACT ORTAL_REDIR tion is enabled, nod="post" action name="auth_page name="au	file chose for the portal ION\$") with a IRL\$". Include otherwise it "type="text "type="pade" type="hidde ype="submit"	page here (le asubmit butto le the "auth_u will always fail CTION\$"> "> word"> ext"> awt"> awt"> avt" avt" avt" avt" avt" avt" avt" avt"	ave blank to keep th n (name="accept") a ser" and "auth_pass" . Example code for t RTAL_REDIRURL\$" > nue" >	e current one nd a hidden f and/or "auth, he form:	). Make sure to ield with nam _voucher' inpi	p include a form e≕redirun″ and ut fields if	

Example de fichier :

```
<html>
<head>
<title>You are being redirected to authentication page</title>
</head>
<body>
<h3>You are being redirected to authentication page</h3>
If you are not redirected, please
<a id="redirect" href="$PORTAL_REDIRURL$">click here</a>
<script type="text/javascript">
var redir = document.getElementById('redirect');
redir.href += window.location.search;
window.location.href="$PORTAL_REDIRURL$" + window.location.search;
</script>
</body>
</html>
```

7. Autoriser le portail captif à acceder à U-Auth et les fournisseurs d'identité de la fédération :

<b>Sense</b>	► System	▶ Interfaces	▶ Firewall	▶ Services	▶ VPN	▶ Status	<ul> <li>Diagnostics</li> </ul>	▶ Gold	▶ Help	밝a pfSense.	entrouvert.lan
	Services Captive porta		portal: e	duspot	lostnames	Vouchers	File Manager		2 6 9	] = 0 = 2	
	IP address	5			Descripti	on					
	176.31.146	.80			u-auth por	tal(https://u-a	.th.dev.entrouvert.or	g)		a 🔉	
	188.165.19	6.219			PSL dev id	p(https://idp-p	sl.dev.entrouvert.org	)		a 🔉	
	195.220.94	.233			idp test fea	deration renat	er(https://test.federat	ion.renater.f	ir)		
	Note: Adding allo page. This	wed IP addresses can be used for a	s will allow IP act web server ser	cess to/from the ving images for	se addresse the portal pa	es through the age or a DNS :	e captive portal withou server on another ne	ut being take twork, for ex	n to the portal kample.	ß	

8. Dans le resolver DNS local rajouter le nom et l'adresse locale du portail captif :

<b>Sense</b>	▶ System	► Interfaces	▶ Firewall	- Services	► VPN	▶ Status	<ul> <li>Diagnostics</li> </ul>	▶ Gold	▶ Help	a pfSense.entrouvert.lan	
	Services	: DNS Re	solver: E	Captive Portal DHCP Relay DHCP Server DHCPv6 Relay					C	86332	
	Edit DNS Res Host	olver entry	Name of the e.g. <i>myhost</i>	DHCPv6 Serv DNS Forward DNS Resolve Dynamic DNS	er/RA ler						
	Domain		Nexamp Domain of th e.g. <i>example</i>	IGMP proxy Load Balance	r						
	IP address		N address o e.g. 192.168	PPPoE Server SNMP UPnP & NAT-I	Nabed::1 PMP						
	Description		You may ent	Wake on LAN er-a description	here for yo	ur reference (r	ot parsed).				
	Aliases		Enter addit Host Dom	ional names for ain Descript	this host.						
	System	▶ Interfaces	Save	Cancel	► VPN	▶ Status	▶ Diagnostics	S Gold	► Hein	Ha of Sense, entrouver t	an

Edit DNS Resolver ent	ry	
Host	Non pfsense Name of the host, without domain part e.g. <i>myhost</i>	
Domain	Sexample.org Domain of the host e.g. example.com	
IP address	N 10.42.0.1 IP address of the host e.g. 192.168.100.100 or fd00:abcd∷1	
Description	You may enter a description here for your reference (not parsed).	
Aliases	Enter additional names for this host.	
	Host Domain Description	

## 2 Test d'authentification

Depuis un poste interne au réseau du portail captif aller sur une page(par exemple http ://perdu.com) :



La page personnalisée, rédirigeant vers U-Auth, sera affichée :

Iceweasel					<b>†</b> -	. a x
https://pfseerdu.com%2F × +						
♦	ō,	☆	Ê	+	⋒	≡
You are being redirected to authentication page						
if you are not redirected, please click here						
1 jou aro not roan occou, prouse <u>onen nor o</u>						

Si l'accès à la plateforme U-Auth a été bien autorisée au niveau du portail captif, la page de votre organisme avec la liste des fournisseurs d'identité sera affichée :

3	U-Auth - Iceweasel	σ×
U-Auth	× \+	
🗲 🔒 http	ps://u-auth.dev. <b>entrouvert.org</b> /pfsense-example?zone=eduspot&redirurl=http% ▼ C ▼ Google 🔍 🙀 自 🖡 🏫	≡
· · ·		
•	Ecole Centrale de Lyon TEST	
•	Ecole Centrale de Nantes	
•	Ecole Nationale Polytechnique d'Alger	
•	ENSA Strasbourg	
•	Ecole Nationale Supérieure de Chimie Paris	
	Ecole Nationale Vétérinaire de Toulouse (ENVT)	
•	Ecole Nationale des Chartes	
•	Ecole des Mines d'Ales	
•	Ecole des Mines de Nantes	Ι Γ
•	Ecole des Transmissions - Cesson Sévigné	
•	Mines-Albi	
•	Ecoles de Saint- Cyr Coëtquidan	
	FNSP TEST	
•	French National Education of Federation - HUB IDP HN02 FER	
	Fédération Éducation-Recherche - IdP de Test	
	GENES IdP test	
	RENATER - 2FA	
	Google Gateway	
	Grenoble INP - Institut polytechnique de Grenoble	
	HEC Paris	
	IDP Alyotech Dev Pelican	
	IDP Alyotech Pelican	
	IDP test for ENVA	
	IDP de test Université de Lorraine	
	IDP test ETRS	
	IDP test mines-nantes	
	IFMA Clermont-Ferrand - Institut Francais de Mecanique Avancee	
	IFSTTAR	
		5.

En choisisant un fournisseur d'identité, également autorisé au niveau du portail captif, la mire de connexion est affichée :

<b>©</b>	Page de connexion - lce	weasel		¢	- @ X
Page de connexion 🗙 🕀					
← A https://test.federation.renater.fr/idp/Authn/Us	erPassword	▼ C Google	🖾 🏠 🗎		≡
TRENATER					
Connexion à uauth					
	> Aide				
Connexion					
logo du service (optionnel) connexion interface for captive portal					
		_			Þ

unight © 2013 Entr'ouvert	113	
Con	Convight ♥ 2013 Entr'ouvert — authentic2 2 :	°ausisht © 2013 Entr'ausant — authantis 2 2 1 13

Une fois authentifié auprès du fournisseur d'identité l'utilisateur est autorisé au niveau du portail captif et est renvoyée vers la page demandée initiallement(dans cet exemple http://perdu.com)

La session utilisateur sera visible dans le dashboard du portail captif :

*Sense	► System ► Inte	erfaces ► Firewall	▶ Services	▶ VPN	▶ Status	▶ Dia	agnostics	5 ▶	Gold	▶ Help		붉ª pfSen	se.entrouvert.lan	
	Status: Dashboard 🖃 🗃											3		
	System Information			Interfaces							$\square$			
	Name	pfSense.entrouvert.lan			🖾 WAN			•	1000baseT <full-duplex></full-duplex>					
	Version	2.2.1-RELEASE (amd64)			(DHCP)			•	10.0.2.15					
		FreeBSD 10.1-RELEASE-p6					+	1000baseT <full-duplex></full-duplex>						
		You are on the latest version.						<u> </u>	10.42.0.1					
	Platform	pfSense	Ser	Services Status										
	СРИ Туре	Intel(R) Core(TM) i5-3230M CPU @ 2.60GHz 02 Hours 43 Minutes 06 Seconds			Service Deceri				serintio		Statuc			
	Uptime				apin	apinger		way Monitoring Daemon		Daemon	Juus	രര		
	Current date/time	Wed Mar 25 13:28:16 C		captiveportal		Captiv	e Porta	al:edusp	eduspot		88			
	DNS server(s)	127.0.0.1 91.121.58.181 87.98.149.171			dhcpd		DHCP Service				CC C			
				ntpd	ntpd NTP clock synd			/nc 🔼			C C			
	Last config change	Wed Mar 25 13:27:29 C	unbound Unbound DN				S Resolv	esolver D		ßŝ				
	State table size	0% (57/98000) Show states			Captive Portal Status IP address MAC address Username									
	MBUF Usage	3% (760/26584)		10.42.0.101 08		08:00:27	:7b:f2:(	f2:00 afaf57825c9147de813651			La682da889a			
	Load average	0 13 0 13 0 09												