

Reverse-proxy

On ajoute un certificat SSL (Wildcard) dans System > Cert. Manager, et dans l'onglet "Certificates".

Search





Search term

Both

SearchClear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

| Name | Issuer | Distinguished Name | In Use | Actions |
|---|-----------------|---|-----------------|---|
| webConfigurator default (5fbd278403e5d) Server Certificate CA: No Server: Yes | self- signed | O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-5fbd278403e5d Valid From: Tue, 24 Nov 2020 14:32:20 -0100 Valid Until: Mon, 27 Dec 2021 14:32:20 -0100 | webConfigurator |     |

+ Add/Sign

Add/Sign a New Certificate

Method

Import an existing Certificate

Descriptive name

Wildcard

Import Certificate

Certificate Type

☒ X.509 (PEM) ☐ PKCS #12 (PFX)









Certificate data

gQFOzcVFSe2P8QqBrSQmbzj9Kc1G1TejfrYsAoQ8Ban
2R5jaBMWtYRnMDnQyF82K
J8cIXK/MK3KI7GjrpKHUdhTk/c5j6QPT1uMrM9mQkC
5
-----END CERTIFICATE-----
Paste a certificate in X.509 PEM format here.

Private key data







-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgqhkiG9w0BAQEFAASCByggSiAgE
AAoIBAQCZGvp5LrqEXBi+
KhSjDXvdRqAC3CG7e+N8Vfo/AstVjo031oFsurKsKSD
vx1vaBSPHjKXTmIdUbQt2
Paste a private key in X.509 PEM format here. This field may remain empty in certain cases, such as when the private key is stored on a PKCS#11 token.

Backends

| | Advanced | Name | Servers | Check | Frontend | Actions |
|--|----------|-------------------|---------|-------|-----------------|---|
| <input type="checkbox"/>  | | www.littoral1.fr | 1 | HTTP | shared-frontend |    |
| <input type="checkbox"/>  | | mail.littoral1.fr | 1 | none | shared-frontend |    |

 Add  Delete  Save

Frontends

| Primary | Shared | On | Advanced | Name | Description | Address | Type | Backend | Actions |
|--|--------|-------------------------------------|---|-----------------|-----------------|---|-------|--|---|
| <input type="checkbox"/>  | | <input checked="" type="checkbox"/> |  | shared-frontend | shared-frontend | 192.168.199.5:443  | https | www.littoral1.fr if(WEB) mail.littoral1.fr if(MAIL) |    |

 Add  Delete  Save

Name

shared-frontend

Description

shared-frontend






Status

Active

External address

Define what ip:port combinations to listen on for incoming connections.

Table

| | Listen address | Custom address | Port | SSL Offloading | Advanced | Actions |
|--|--|----------------|------|-------------------------------------|----------|---|
| <input type="checkbox"/>  | WAN address (IPv4)  | | 443 | <input checked="" type="checkbox"/> | |    |

NOTE: You must add a firewall rules permitting access to the listen ports above.

If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define [Virtual IP](#) addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (,). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Max connections

Sets the maximum amount of connections this frontend will accept, may be left empty.

Type

http / https(offloading)

This defines the processing type of HAProxy, and will determine the available options for ssl checks and also several other options

Default backend, access control lists and actions

Access Control lists

Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

| Table | | | | | | |
|--------------------------|------|---------------|----|-----|-------------------|---------|
| | Name | Expression | CS | Not | Value | Actions |
| <input type="checkbox"/> | WEB | Host matches: | no | no | www.littoral1.fr | |
| | | | | | | |
| <input type="checkbox"/> | MAIL | Host matches: | no | no | mail.littoral1.fr | |
| | | | | | | |

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld wil not be the same as WWW.domain.TLD

- 'Not' makes the match if the value given is not matched

Example:

| Name | Expression | CS | Not | Value |
|--------------|------------------------------|----|-----|--------------------|
| Backend1acl | Host matches | | | www.yourdomain.tld |
| addHeaderAcl | SSL Client certificate valid | | | |

acl's with the same name will be 'combined' using OR criteria.

For more information about ACLs please see [HAProxy Documentation](#) Section 7 - Using ACLs

NOTE Important change in behaviour, since package version 0.32

-acl's are no longer combined with logical AND operators, list multiple acl's below where needed.

-acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

Actions

Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

| Table | | | |
|--------------------------|----------------------------|------------|---------------------|
| | Action | Parameters | Condition acl names |
| <input type="checkbox"/> | Use Backend | See below | WEB |
| | backend: www.littoral1.fr | | |
| <input type="checkbox"/> | Use Backend | See below | MAIL |
| | backend: mail.littoral1.fr | | |

Example:

| Action | Parameters | Condition |
|-------------------------|--|--------------|
| Use Backend | Website1Backend | Backend1acl |
| http-request header set | Headername: X-HEADER-ClientCertValid New logformat value: YES | addHeaderAcl |

Default Backend

None

the time (in milliseconds) we accept to wait for data from the client, or for the client to accept data (default 30000).

Use "forwardfor" option

☐ Use "forwardfor" option.

The "forwardfor" option creates an HTTP "X-Forwarded-For" header which contains the client's IP address. This is useful to let the final web server know what the client address was. (eg for statistics on domains)

Use "httpclose" option

http-keep-alive (default)

By default HAProxy operates in keep-alive mode with regards to persistent connections: for each connection it processes each request and response, and leaves the connection idle on both sides between the end of a response and the start of a new request.

Bind pass thru

NOTE: paste text into this box that you would like to pass behind each bind option.

Advanced pass thru

NOTE: paste text into this box that you would like to pass thru in the frontend.

SSL Offloading

Note SSL Offloading will reduce web servers load by maintaining and encrypting connection with users on internet while sending and retrieving data without encryption to internal servers. Also more ACL rules and http logging may be configured when this option is used. Certificates can be imported into the pfSense "Certificate Authority Manager" Please be aware this possibly will not work with all web applications. Some applications will require setting the SSL checkbox on the backend server configurations so the connection to the webserver will also be a encrypted connection, in that case there will be a slight overall performance loss."

SNI Filter

Specify a SNI filter to apply below SSL settings to specific domain(s), see the "crt-list" option from haproxy for details.
EXAMPLE: *.securedomain.tld !public.securedomain.tld

Certificate

Choose the cert to use on this frontend.

- ☐ Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)
- ☐ Add ACL for certificate Subject Alternative Names.

OCSP

- ☐ Load certificate ocsp responses for easy certificate validation by the client.
A cron job wil update the ocsp response every hour.

Additional certificates

Which of these certificate will be send will be determined by haproxys SNI recognition. If the browser does not send SNI this will not work properly. (IE on XP is one example, possibly also older browsers or mobile devices).

Table

| Certificates | Actions |
|--------------|---------|
|--------------|---------|

Revision #4

Created 17 March 2021 10:50:51 by Khroners

Updated 5 July 2021 15:28:36 by Khroners