

How to enable the HAProxy statistics page in OPNsense

Step 1: Edit Global Settings

In the left-hand menu, go to **Services** , select **HAProxy** and then and then **Settings**.

- Under the **Settings** tab, locate the **Global Parameters**
- Enable ' **Advanced Mode** ' on the top left of the page
- Add or modify the following configuration line in the “**Custom Options**” field (on the bottom of the picture):

```
stats socket /var/run/haproxy.socket group proxy mode 775 level admin
```

This enables a UNIX socket for administrative purposes.

▼ Global Parameters

i Run as root

☐

Enable or disable HAProxy running as user root. Enabling this option is strongly discouraged.

NOTE: Running as user root could be a security issue but it may be required by some features.

i HAProxy threads

4

Number of threads to create for each HAProxy process.

i Maximum connections

5000

Sets the maximum number of concurrent connections per HAProxy process.

NOTE: Consider raising the settings for `kern.maxfiles` and `kern.maxfilesperproc` in [System: Settings: Tunables](#), otherwise HAProxy will fail to open the specified number of connections.

i DNS prefer IP family

IPv4

This option allows to choose which IP family is preferred when resolving DNS names. This is useful when IPv6 or IPv4 is not available. It solves a common issue with OCSP updates.

i Verify SSL Server Certificates

no preference [default]

This enforces a certain behavior for SSL verify on servers, ignoring per-server settings. If set to 'enforce verify', server certificates are verified. If set to 'disable verify', server certificates are not verified. The default is 'no preference' to only use per-server configurations and not enforce a global default for all servers.

i Maximum SSL DH Size

4096

Sets the maximum size of the Diffie-Hellman parameters used for generating the ephemeral/temporary Diffie-Hellman key in case of DHE key exchange (default is 1024).

NOTE: Higher values will increase the CPU load. For more information about the `"tune.ssl.default-dh-param"` option please see the HAProxy Documentation.

i Buffer size

16384

Change the buffer size (in bytes). Lower values allow more sessions to coexist in the same amount of RAM, and higher values allow some applications with very large cookies to work. The default value is 16384.

NOTE: It is strongly recommended not to change this from the default value, as very low values will break some services such as statistics, and values larger than default size will increase memory usage, possibly causing the system to run out of memory.

i Maximum RAM per LUA process

0

Sets the maximum amount of RAM in megabytes per process usable by Lua. By default it is zero which means unlimited. It is important to set a limit to ensure that a bug in a script will not result in the system running out of memory.

i Spread checks

2

Add some randomness in the check interval between 0 and +/- 50%. A value between 2 and 5 seems to show good results. The default value is 0 (disabled).

i Enable old bogus PROXY v2 implementation

☐

A bug in the PROXY protocol v2 implementation was present in HAProxy up to version 2.1. Enabling this option reverts this old buggy behaviour.

i Custom options

stats socket /var/run/haproxy.socket group proxy mo ...

Step 2: Configure Statistics in Frontend Settings

- Go to **Virtual Servers** in the Top menu
- Click the + sign and add a new Public Service: '**StatsFrontend**'
- In this frontend, configure it as follows:
 - Set Name: **StatsFrontend**
 - Set Listen Addressess: set to local IP address of OPNsense (e.g. 192.168.2.1) with the default port 8822
 - Set Type to default **HTTP/HTTPS (SSL offloading) [default]**
 - Scroll all the way down to “**Advanced Settings**”, add these lines in the “**Option Pass-through**” field:

```
stats enable
stats uri /haproxy?stats
stats realm Haproxy\ Statistics
stats auth admin:password123
```

Replace **admin** with your desired username and **password** with a strong password.

- Click on “Save” and then apply changes by clicking on “Apply”.

The length of the period over which the average is measured. It reports the average HTTP request rate over that period, in requests per period. Defaults to milliseconds. Optionally the unit may be specified as either "d", "h", "m", "s", "ms" or "us".

HTTP error rate period

The length of the period over which the average is measured. It reports the average HTTP request error rate over that period, in requests per period. Defaults to milliseconds. Optionally the unit may be specified as either "d", "h", "m", "s", "ms" or "us".

Bytes in rate period

The length of the period over which the average is measured. It reports the average incoming bytes rate over that period, in bytes per period. Defaults to milliseconds. Optionally the unit may be specified as either "d", "h", "m", "s", "ms" or "us".

Bytes out rate period

The length of the period over which the average is measured. It reports the average outgoing bytes rate over that period, in bytes per period. Defaults to milliseconds. Optionally the unit may be specified as either "d", "h", "m", "s", "ms" or "us".

▼ **Advanced settings**

Option pass-through

```
stats enable
stats uri /haproxy?stats
stats realm Haproxy\ Statistics
stats auth admin:password|
```

These lines will be added to the HAProxy frontend configuration.

▼ **Rules**

Select Rules

✖ Clear All 📄 Copy 📄 Paste 📄 Text

Step 3: Configure Firewall Rules

1. Allow Access to the Statistics Port:

- Navigate to **Firewall > Rules > LAN**
- Create a new rule with these parameters:
 - Action: **Pass**
 - Protocol: **TCP**
 - Destination: **This Firewall**
 - Destination Port Range: **Other and the 8822**
 - Description: **Access the Statistics page**
 - Leave everything else to the default values
 - Save the rule and click on "Apply Changes".

Firewall: Rules: LAN

Edit Firewall rule

full help

<div><div></div><div>Action</div></div>	<div>Pass</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</div>
<div><div></div><div>Disabled</div></div>	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
<div><div></div><div>Quick</div></div>	<div><input checked="" type="checkbox"/> Apply the action immediately on match.</div> <div>If a packet matches a rule specifying quick, then that rule is considered the last matching rule and the specified action is taken. When a rule does not have quick enabled, the last matching rule wins.</div>
<div><div></div><div>Interface</div></div>	<div>LAN</div> <div>Choose on which interface packets must come in to match this rule.</div>
<div><div></div><div>Direction</div></div>	<div>in</div> <div>Direction of the traffic. Traffic IN is coming into the firewall interface, while traffic OUT is going out of the firewall interface. In visual terms: [Source] -> IN -> [Firewall] -> OUT -> [Destination]. The default policy is to filter inbound traffic, which means the policy applies to the interface on which the traffic is originally received by the firewall from the source. This is more efficient from a traffic processing perspective. In most cases, the default policy will be the most appropriate.</div>
<div><div></div><div>TCP/IP Version</div></div>	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to</div>
<div><div></div><div>Protocol</div></div>	<div>TCP</div> <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.</div>
<div><div></div><div>Source / Invert</div></div>	<div><input type="checkbox"/> Use this option to invert the sense of the match.</div>
<div><div></div><div>Source</div></div>	<div>any</div>
<div>Source</div>	<div>Advanced</div> <div>Show source address and port range</div>
<div><div></div><div>Destination / Invert</div></div>	<div><input type="checkbox"/> Use this option to invert the sense of the match.</div>
<div><div></div><div>Destination</div></div>	<div>This Firewall</div>
<div><div></div><div>Destination port range</div></div>	<div><div>from:</div><div>(other)</div><div>8822</div></div> <div><div>to:</div><div>(other)</div><div>8822</div></div> <div>Specify the port or port range for the destination of the packet for this mapping.</div>

OPNsense (c) 2014-2025 Deciso B.V.

Step 4: Test Access to the Statistics Page

1. Open a web browser from a device allowed by your firewall rules.
2. Enter the URL for accessing statistics, such as:

```
http://192.168.2.1:8822/haproxy?stats
```

Enter the username and password you configured earlier when prompted.

If everything is configured correctly, you should see HAProxy's statistics page displaying real-time data about connections, backends, frontends, etc.

Statistics Report for pid 64479

> General process information

pid = 64479 (process #1, rbgproc = 1, nbthread = 4)
uptime = 0d 0h0m24s; warnings = 0
system limits: memmax = unlimited; ulimit-n = 10037
maxsock = 10037; maxconn = 5000; reached = 0; maxpipes = 0
current conns = 1; current pipes = 0/0; conn rate = 0/sec; bit rate = 0.000 kbps
Running tasks: 0/23; idle = 100 %

active UP
active UP, going down
active DOWN, going up
active or backup DOWN
active or backup DOWN for maintenance (MAINT)
active or backup SOFT STOPPED for maintenance

backup UP
backup UP, going down
backup DOWN, going up
not checked
Note: "NOLE77DRAIN" = UP with load-balancing disabled.

Display option:

Scope:

Hide **DOWN** servers
Refresh now
CSV export
JSON export (schema)

External resources:

Primary site
Updates (v2.8)
Online manual

flutleggen

	Queue			Session rate			Sessions					Bytes		Denied		Errors		Warnings		Server											
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dvntme	Thrtle	
Frontend				0	0	-	0	0		5 000	0		0	0	0	0	0	0				OPEN									

StatsFrontend

	Queue			Session rate			Sessions					Bytes		Denied		Errors		Warnings		Server											
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dvntme	Thrtle	
Frontend				0	1	-	1	1		5 000	1		420	469	0	0	0	0				OPEN									

flutleggen

	Queue			Session rate			Sessions					Bytes		Denied		Errors		Warnings		Server											
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dvntme	Thrtle	
flutleggen	0	0	-	0	0		0	0		2000	0	0	?	0	0	0	0	0	0	0	0	no check		1/1	Y	-					-
Backend	0	0		0	0		0	0		500	0	0	?	0	0	0	0	0	0	0	0	25s UP		1/1	1	0		0	0s		

local statistics

	Queue			Session rate			Sessions					Bytes		Denied		Errors		Warnings		Server											
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dvntme	Thrtle	
Frontend				0	0	-	0	0		5 000	0		0	0	0	0	0	0				OPEN									
Backend	0	0		0	0		0	0		500	0	0	?	0	0	0	0	0	0	0	0	25s UP		0/0	0	0		0			

Revisie #5
Gemaakt: 24 januari 2025 16:05:27 door Gert
Bijgewerkt: 24 januari 2025 16:56:19 door Gert