

OPNSense

- [HAProxy Simple Configuration for local webserver](#)
- [Adguard Home communications error to 127.0.0.1#53: connection refused](#)
- [Disable IPv6 in OPNSense](#)
- [How to enable the HAProxy statistics page in OPNsense](#)

HAProxy Simple Configuration for local webserver

Parameters for this setup

Local webserver is on ip address 192.168.1.200 and uses port 80

Step 1: Define a Real server

- Name: **anything** you like to recognize the webserver
- IP address: The IP address of the internal webserver e.g. **192.168.1.200**
- Port: **80**
- SSL: **disable**

Edit Backend Pool



advanced mode

full help

Enabled ☒

Name

Description

Mode

Balancing Algorithm

Servers
 Clear All Copy Paste Text

FastCGI Application

Resolver Options
 Clear All Copy Paste Text

Enable Health Checking ☒

Health Checking

Health Monitor

Log Status Changes ☐

E-Mail Alert

HTTP(S) settings

Enable HTTP/2 ☒

HTTP/2 without TLS ☐

Advertise Protocols (ALPN)
 Clear All Copy Paste Text

Forwarded header (RFC7239) ☐

Forwarded header parameters
 Clear All Copy Paste Text

Cancel

Save

Edit Backend Pool

X-Forwarded-For header
☐

Persistence

Persistence type
Stick-table persistence [default]

Stick-table persistence

Table type
Source-IP [default]

Stored data types
Nothing selected

Clear All
Select All

Cookie name

Cookie length

Basic Authentication

Enable
☐

Allowed Users
Type username or choose from list.

Clear All
Select All

Allowed Groups
Type group or choose from list.

Clear All
Select All

Tuning Options

Retries

Rules

Select Rules

Clear All
Copy
Paste
Text

Error Messages

Select Error Messages
Choose error messages.

Clear All
Select All

Cancel

Save

Step 2: Define a condition:

- o Name: **anything** you like
- o Condition: **Host contains** or you can use any other condition to match like **Host matches** and use the full url.
- o Host string = **Anything to recognize the URL** or the full url in case of host matches.

Edit Condition ✕

[full help](#)

Name

Description

▼ **Condition**

Condition type

Negate condition ☐

Case-sensitive ☐

▼ **Parameters**

Host Contains

Step 3: Define a rule

- Name: **anything** you like
- Select Conditions: **Select the webserver** from the dropdown menu
- Under HAProxy function > Execute function: **Use specified Backend Pool**
- Use backend pool: **Select the backend Pool** from the drop down menu

The screenshot shows the 'Edit Rule' dialog box in the HAProxy configuration interface. The dialog has a title bar with 'Edit Rule' and a close button. A 'full help' link is in the top right. The form contains several sections: 'Name' with the value 'ffuitleggen'; 'Description' which is empty; 'Optional condition' section containing 'Test type' (IF [default]), 'Select conditions' (ffuitleggen) with 'Clear All' and 'Select All' links, and 'Logical operator for conditions' (AND [default]); 'HAProxy function' section with 'Execute function' (Use specified Backend Pool); and 'Parameters' section with 'Use backend pool' (ffuitleggen). 'Cancel' and 'Save' buttons are at the bottom right.

| | |
|---------------------------------|----------------------------|
| Edit Rule | |
| full help | |
| Name | ffuitleggen |
| Description | |
| Optional condition | |
| Test type | IF [default] |
| Select conditions | ffuitleggen |
| * Clear All ✓ Select All | |
| Logical operator for conditions | AND [default] |
| HAProxy function | |
| Execute function | Use specified Backend Pool |
| Parameters | |
| Use backend pool | ffuitleggen |
| Cancel Save | |

Step 4: Define a Virtual Service

Under Public Service:

- Name: **anything** you like
- Listen addresses: **0.0.0.0:443** (TAB)
- Enable SSL offloading: **Checked**
- Default backend pool: **Select from dropdown menu** (TAB)
- Certificate: **your Let's Encrypt certificate**
- Under Advanced settings:
 - Select rules: **The rule you made earlier**

Edit Public Service



advanced mode

full help

Enabled ☒

Name

Description

Listen Addresses

Clear All Copy Paste Text

Type

Default Backend Pool

Enable SSL offloading ☒

SSL Offloading

Certificates

Clear All Copy Paste Text

Default certificate

Enable Advanced settings ☐

Client Certificate Auth

Enable ☐

Verification

Certificate Authorities

Clear All Select All

Certificate Revocation Lists

Clear All Select All

HTTP(S) settings

Enable HTTP/2 ☒

HTTP/2 without TLS ☐

Cancel

Save

Edit Public Service



Advertise Protocols (ALPN)

HTTP/2 × HTTP/1.1 ×

✖ Clear All ✂ Copy 📄 Paste 📄 Text

X-Forwarded-For (DEPRECATED)

☐

Basic Authentication

Enable

☐

Allowed Users

Type username or choose from list.

✖ Clear All ✔ Select All

Allowed Groups

Type group or choose from list.

✖ Clear All ✔ Select All

Tuning Options

Maximum Connections

Logging Options

Detailed Logging

☐

Stickiness table

Table type

None

Stored data types

Nothing selected

✖ Clear All ✔ Select All

Advanced settings

Rules

Select Rules

ffuitleggen ×

✖ Clear All ✂ Copy 📄 Paste 📄 Text

Error Messages

Select Error Messages

Choose error messages.

Cancel

Save

Adguard Home communications error to 127.0.0.1#53: connection refused

When you **cannot update OPNsense** and you see an error in a SSH session when you try to run:

```
root@OPNsense:~ # dig @127.0.0.1 -p 53 google.com
```

```
dig @127.0.0.1 -p 53 google.com
```

You probably have a wrong binding in the Adguard config file.

To solve this issue:

```
nano AdGuardhome.yaml
```

```
cd /usr/local/AdGuardHome
```

Change the bind (from a local ip address) to:

dns:

bind_hosts:

- 0.0.0.0

Then restart Adguard Home

Disable IPv6 in OPNSense

Set IPv6 on all interfaces on 'None' and also remove the 'Allow IPv6' vinkje.

The screenshot shows the OPNSense web interface. The left sidebar contains the navigation menu with the following items: Lobby, Reporting, System, Interfaces, [LAN], [WAN], [WAN_IPTV], Assignments, Overview, Settings (selected), Neighbors, Virtual IPs, Wireless, Point-to-Point, Other Types, Diagnostics, Firewall, VPN, Services, Power, and Help. The main content area is titled 'Interfaces: Settings'. At the top, a blue message box states 'The changes have been applied successfully.' Below this, the 'Network Interfaces' section is displayed. It contains the following settings:

| Setting | Value |
|-------------------------|---|
| Hardware CRC | <input checked="" type="checkbox"/> Disable hardware checksum offload |
| Hardware TSO | <input checked="" type="checkbox"/> Disable hardware TCP segmentation offload |
| Hardware LRO | <input checked="" type="checkbox"/> Disable hardware large receive offload |
| VLAN Hardware Filtering | Disable VLAN Hardware Filtering |
| ARP Handling | <input type="checkbox"/> Suppress ARP messages |
| Allow IPv6 | <input type="checkbox"/> Allow IPv6 |

Below the 'Network Interfaces' section is the 'IPv6 DHCP' section. It contains the following settings:

| Setting | Value |
|------------------------|--------------------------|
| Prevent release | <input type="checkbox"/> |
| Log level | Standard |
| DHCP Unique Identifier | [Empty field] |

Below the 'DHCP Unique Identifier' field, there is a dropdown menu with the following options:

- Insert the existing DUID
- Insert a new LLT DUID
- Insert a new LL DUID
- Insert a new UUID DUID
- Insert a new EN DUID
- Clear the existing DUID

A 'Save' button is located at the bottom of the 'IPv6 DHCP' section. At the very bottom of the page, a note states: 'This will take effect after you reboot the machine or reconfigure each interface.'

Remove also the 'Allow IPv6' rule in de firewall rules:

- Lobby
- Reporting
- System
- Interfaces
- Firewall
 - Aliases
 - Automation
 - Categories
 - Groups
 - NAT
 - Rules
 - Floating
 - LAN
 - Loopback
 - WAN
 - WAN_IPTV
 - Shaper
 - Settings
 - Log Files
 - Diagnostics
- VPN
- Services
- Power
- Help

Firewall: Rules: LAN

Select category

Inspect

The changes have been applied successfully.

| | Protocol | Source | Port | Destination | Port | Gateway | Schedule | Description | |
|---|-----------|------------------|------|-----------------|-------------------|---------|----------------|---------------------------------------|-------------|
| Automatically generated rules | | | | | | | | | |
| | IPv4 IGMP | LAN net | * | 224.0.0.0/8 | * | * | * | LAN INBOUND IGMP, incl. allow options | |
| | IPv4 * | LAN net | * | 213.75.112.0/21 | * | * | * | IPTV | |
| | IPv4 * | LAN net | * | * | * | * | * | Default allow LAN to any rule | |
| pass | | | | | | | log | in | first match |
| pass (disabled) | | block | | | reject | | log (disabled) | out | last match |
| | | block (disabled) | | | reject (disabled) | | | | |
| Active/Inactive Schedule (click to view/edit) | | | | | | | | | |
| Alias (click to view/edit) | | | | | | | | | |
| LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default. | | | | | | | | | |

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

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.

HAProxy threads

4

Number of threads to create for each HAProxy process.

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.

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.

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.

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.

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.

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.

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).

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.

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.<br/>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] -&gt; IN -&gt; [Firewall] -&gt; OUT -&gt; [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.<br/>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 | Dwntme | 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 | Dwntme | 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 | Dwntme | 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    | 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 | Downtme | 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    | 0      | 25s UP |         | 0/0  | 0   | 0   |     | 0   |         |        |  |