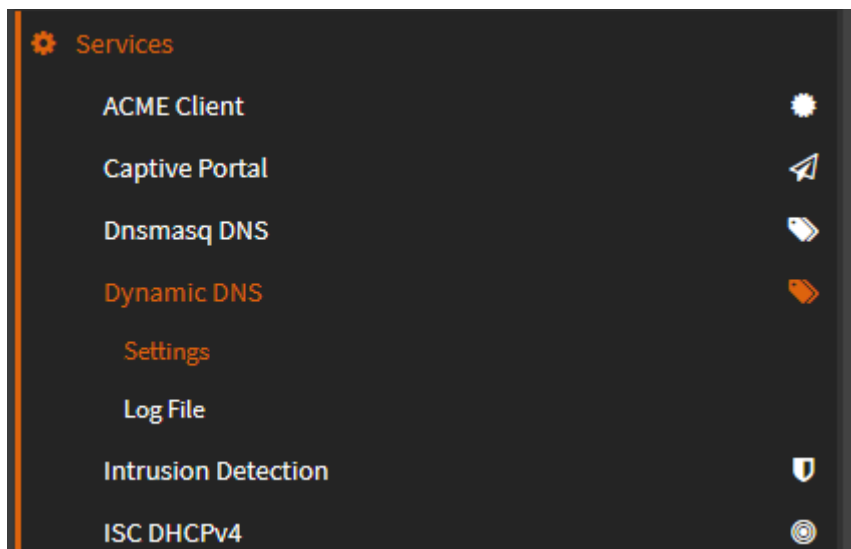


# Cloudflare DDNS

If you have a Dynamic WAN IP, you'll need to set up some sort of DDNS client. Most ISPs use Dynamic IPs with residential customers, so this is pretty common and there are multiple options for working around this. I currently manage my domains with Cloudflare, so I'll be using their DDNS so I can have all my management under 1 provider. Setting this up is fairly simple!

First, make sure the os-ddclient plugin is installed on your OPNsense firewall. Once installed, navigate to Services ---> Dynamic DNS ---> Settings:



Next, select the "+" icon to add an account.

Edit Account

advanced mode

full help

Enabled

☒

Description

Service

aws

Username

Password

Zone

Hostname(s)

Clear All

Copy

Paste

Text

TTL

300

Check ip method

dyndns

Interface to monitor

None

Check ip timeout

10

Force SSL

☒

Cancel

Save

Open up a web browser and create an A Record with your domain registrar for a subdomain. On Cloudfare its fairly simple. Navigate to your DNS records, and create a new record:

DNS management for

DNS Setup: Full

Import and Export

Dashboard Display Settings

Review, add, and edit DNS records. Edits will go into effect once saved.

Search DNS Records

Add filter

Search

Add record

[name] points to [IPv4 address] and has its traffic proxied through Cloudflare.

Type

A

Name (required)

IPv4 address (required)

Proxy status

☒ Proxied

TTL

Auto

Record Attributes

Documentation

The information provided here will not impact DNS record resolution and is only meant for your reference.

Comment

Enter your comment here (up to 100 characters).

Cancel

Save

- Enter a name for your subdomain, and any IP address. The IP you enter doesn't matter as this record will be updated with your WAN IP automatically.
- Make sure you turn Proxy off

Your final settings should look like this:

DNS management for [REDACTED]

Review, add, and edit DNS records. Edits will go into effect once saved.

DNS Setup: Full ⓘ[Import and Export](#) ▼ ⚙️ [Dashboard Display Settings](#)

Search DNS Records

▼ Add filter

Q

Search

+ Add record

example[REDACTED].com points to 192.168.1.1.

Type

A ▼

Name (required)

example ▲ ▼  
Use @ for root

IPv4 address (required)

192.168.1.1

Proxy status

☒ DNS only

TTL

Auto ▼

Record Attributes [Documentation](#)

The information provided here will not impact DNS record resolution and is only meant for your reference.

Comment

Enter your comment here (up to 100 characters).

Cancel

Save

With this record saved, navigate to your API tokens and generate a new API token. Navigate to Overview in Cloudflare, then scroll down and select "Get API token". On the next page, select create token:

API Tokens

Manage access and permissions for your accounts, sites, and products

Create Token

Use the "Edit zone DNS" template and configure the following:

## Create Token

Token name: Edit zone DNS [✎](#)

### Permissions

Select edit or read permissions to apply to your accounts or websites for this token.

Zone ▼	DNS ▼	Edit ▼	✕
Zone ▼	DNS ▼	Read ▼	✕

[+ Add more](#)

### Zone Resources

Select zones to include or exclude.

Include ▼	Specific zone ▼	Select... ▼
-----------	-----------------	-------------

[+ Add more](#)

### Client IP Address Filtering

Select IP addresses or ranges of IP addresses to filter. This filter limits the client IP addresses that can use the API token with Cloudflare. By default, this token will apply to all addresses.

Operator	Value
Select item... ▼	e.g. 192.168.1.88 ▼

[+ Add more](#)

### TTL

Define how long this token will stay active.

Start Date → End Date
-----------------------

- Enter a name for the token
- Add another permission as Zone - DNS - Read
- Under zone resrouces configure Include - Specific Zone - Select the domain you have the A Record configured with
- After creating the token, save it somewhere! You will not be able to view this token again!

With your A Record configured, and API token in hand, you can now go back to the OPNsense Page:

Edit Account

advanced mode

full help

Enabled

☒

Description

Service

aws

Username

Password

Zone

Hostname(s)

Clear All

Copy

Paste

Text

TTL

300

Check ip method

dyndns

Interface to monitor

None

Check ip timeout

10

Force SSL

☒

Cancel

Save

- Enable the account
- Give it a Description or name
- Select Cloudflare under Service
- Keep username blank
- Enter your API token as the password
- For zone, enter your domain name
  - example.com
- For Hostname, enter your FQDN
  - vpn.example.com
- For Check IP method, select ip4only.me
- Force SSL, then save configurations

Edit Account

advanced mode

full help

Enabled

☒

Description

WGVPN

Service

cloudflare

Username

Password

Wildcard

☐

Zone

Hostname(s)

Clear All

Copy

Paste

Text

Check ip method

ip4only.me

Interface to monitor

WAN

Check ip timeout

10

Force SSL

☒

Cancel

Save

Save your settings and apply the new configurations. Select the refresh icon and your WAN IP should now be updated!

SERVICES: DYNAMIC DNS: SETTINGS								
Accounts								
General settings								
Enabled	Service	Hostnames	Username	Interface	Current IP	Updated	Description	Commands
<input checked="" type="checkbox"/>	cloudflare			WAN		2024-04-01T04:27:44+00:00	WGVPN	
Showing 1 to 1 of 1 entries								

Check your DNS A Record to see if your WAN IP has updated. It should automatically update. You can now get your WAN IP from this subdomain, as it'll automatically update. To ensure it automatically updates, I've created a cron job in my router to check for changes in my IP every 6 hours and update if necessary.

Revision #3

Created 1 April 2024 19:47:46 by Austin

Updated 1 April 2024 20:13:33 by Austin