

Open Dns

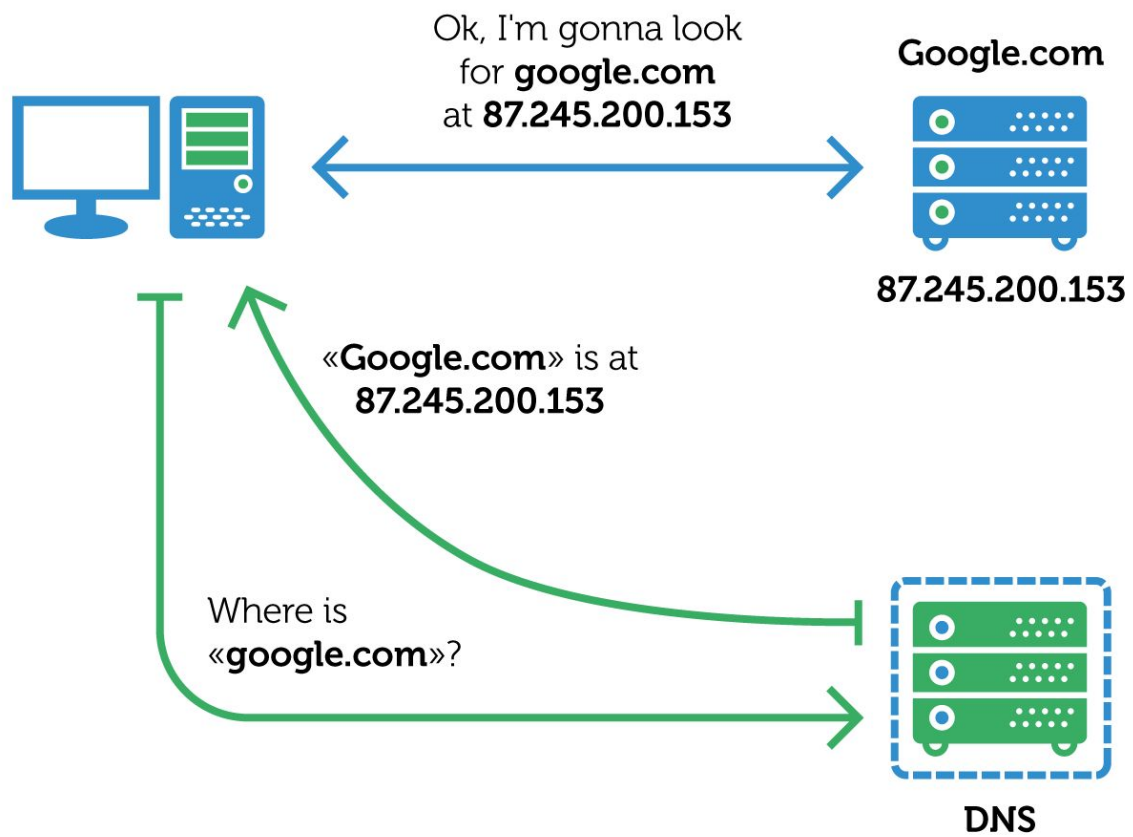


Summary

1. Introduction
2. Setting Up

1. Introduction to DNS

Domain Name System (DNS) is a service able to translate a domain name into IP addresses.

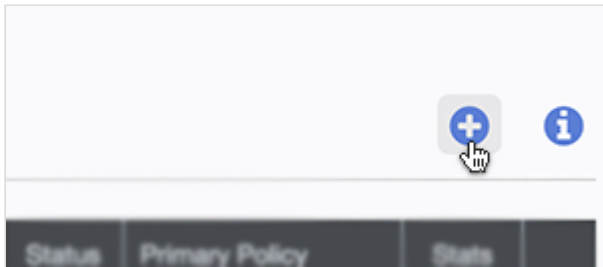


© 2016 AO Kaspersky Lab. All Rights Reserved.

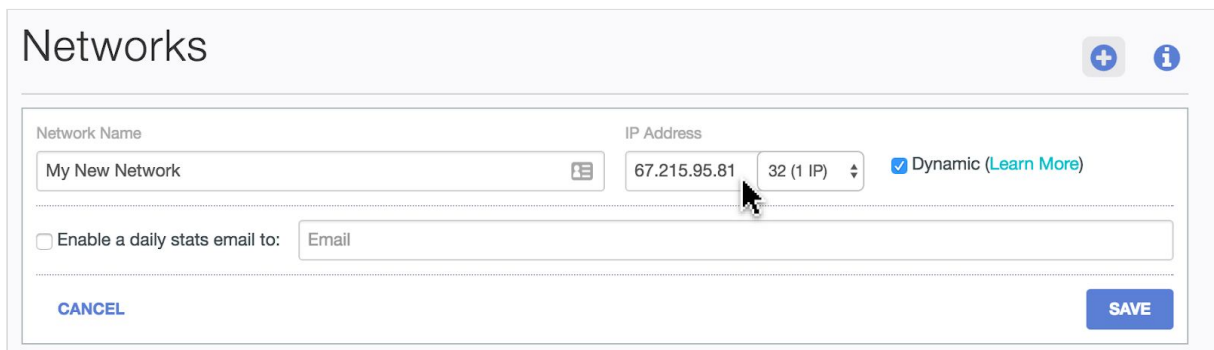
2. Setting up Cisco Umbrella (new OpenDns)

2.1 Connexion

To add a Network Identity, go to Configuration -> Identities -> Networks .
Click "Add a new network," and choose a descriptive name.



Enter the public IP address of the network along with the subnet mask, usually a /32 subnet.

A screenshot of the 'Networks' configuration form in the Cisco Umbrella interface. The form has a light gray header with the title 'Networks' and two icons (a plus in a circle and an information icon in a circle). The form itself is white with a gray border. It contains the following fields: 'Network Name' with the text 'My New Network' and a calendar icon; 'IP Address' with the text '67.215.95.81' and a dropdown menu showing '32 (1 IP)'; a checkbox labeled 'Dynamic' with the text '(Learn More)' next to it; a checkbox labeled 'Enable a daily stats email to:' followed by an 'Email' input field; a blue 'CANCEL' button at the bottom left; and a blue 'SAVE' button at the bottom right.

Once the service accepts your IP address, the network will appear in the list at Configuration -> Identities -> Networks . The network will be red for the next 90 minutes. After that time, if the network has sent a DNS request to Cisco Umbrella, the status would become green and the network will be activated.

| Networks | | | | | | |
|-----------------------------------|--------------|-------------------------------|----------------|-------|--|--|
| <div>Search the Networks...</div> | | | | | | |
| Name | IP | Status | Policy | Stats | | |
| My New Network | 67.215.95.81 | Active over the past 24 hours | Default Policy | | | |

Your network is now configured. Next, point your network's DNS traffic to the Cisco Umbrella.

Change your DNS server address for this addresses:

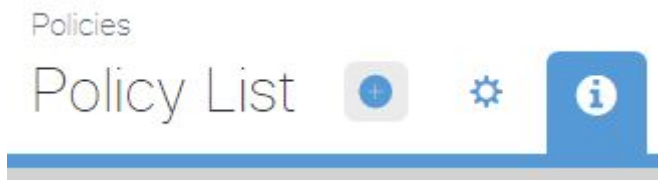
208.67.222.222 and 208.67.220.220

While connected to the network that you've just configured, browse to <http://welcome.opendns.com> . If you have successfully set your public DNS to the Cisco Umbrella servers, you will see this confirmation page.



Welcome to OpenDNS!
Your Internet is safer, faster, and smarter
because you're using OpenDNS.
Thank you!

2.2 Security policy



Go to Configuration -> Policies and click the icon to create a new policy or select *Default Policy*.

Select any or all of the identities that you've created in the previous steps. If you chose *Default Policy*, all identities will be selected.

1

*** New Policy ***

Impacting
0 Identities

Category Setting

Security Setting

1. Select Identities

2. Select Policy Settings

3. Select Block Page Settings

4. Set Policy Details

All Identities

☐ Mobile Devices (0)

☐ Network Devices (0)

☒ Networks (1)

☐ Roaming Computers (0)

All Networks

CANCEL

NEXT

You can create new settings or edit the defaults for the following setting types:

- *Category Settings* - these settings filter types of content based on your Organization's acceptable use policies.
- *Security Settings* - these settings set the types of security settings you'd like to have to protect yourself on the internet.
- *Destination Lists* - If you have particular domains you'd like to allow or block, add them to a destination list. There are two by default, *block* or *allow*, and you can create more to organize groups of domains.

1

*** New Policy ***

Impacting
0 Identities

Category Setting

Security Setting

1. Select Identities


2. Select Policy Settings

3. Select Block Page Settings

4. Set Policy Details

Category setting to enforce:


add new setting

 Default Settings

or Whitelist-only mode ?

Security setting to enforce:


add new setting

 Default Settings


Domain lists to enforce:


add new domain list

Select from existing domain list


 Global Block List

☒ block



 Global Allow List

☒ allow



CANCEL

PREVIOUS

NEXT

You can customize the block page appearance and optionally choose to allow people the ability to bypass sites that were blocked by adding bypass users or codes.

1

*** New Policy ***

Impacting
0 Identities

Category Setting

Security Setting

1. Select Identities


2. Select Policy Settings

3. Select Block Page Settings

4. Set Policy Details

Block Page setting to enforce:

add new setting

 Default Settings

Users that can bypass block pages:

add user

No bypass user found.

Codes that can bypass block pages:

add code

No bypass code found.

Please note that "redirect users to a URL" will be disabled if one or more bypass users or codes is applied to this policy.

CANCEL

PREVIOUS

NEXT

Give your policy a descriptive to remember name easier. For now, leave logging on to make sure that everything is working as expected. You can return to this page at any time to change log settings.

1

*** New Policy ***

Impacting
0 Identities

Category Setting

Security Setting

1. Select Identities

2. Select Policy Settings

3. Select Block Page Settings

4. Set Policy Details

Policy description:

San Francisco Office

Request Logging:

Logging enabled

All content & security requests will be reported and alerted on.

CANCEL

PREVIOUS

SAVE