NTOPNG - Network Analysis Dashboard

https://www.youtube.com/embed/sJkLmjaj02E

NTOPNG (I rponounce it N-Top-N-G) is a browser based server application you can run in Docker. By setting it up properly, it can scan your entire network and provide analytical data back about traffic patterns adn levels from different machines or sub-networks within your network.

Whether you're an IT admin, or an at-home self-hoster, viewing, analyzing, and understanding your network traffic patterns can help keep your networks more secure by detecting anomolies and potential intrusion quickly, as well as helping to close security gaps.

Installing NTOPNG in Docker

Install Docker

I have several posts that go through the steps of installing Docker and Docker-Compose on Ubuntu based systems for 18.04 and 20.04. If you don't have docker setup already, I use Docker_CE (not Docker.io) to run all of my docker containers. I recommend you go back to those posts and get Docker installed at the very least. It's truly basic terminal commands, and should only take 5 or so minutes. Click the link below, or right click and open it in a new tab or window to reference it as you continue.

https://shownotes.opensourceisawesome.com/putting-it-all-together/

Install NTOPNG

Now that you've got Docker installed, it's time to get into the NTOPNG installation inside of Docker. Not to worry, while most docker containers are "confined" to their container and docker networks, this one is going to be able to access the NIC (Network Interface Card) we specify when running the command to install it and start it up. So let's go identify our active network device name.

In Linux you have a couple of commands that may give you results. The newer command is

```
ip addr show
```

This will list out all of your network interfaces on the device. Look for the one with your normal network IP (for home networks often 192.168.x.x or sometimes 10.0.x.x, etc). You may have two different cards if you have both an ethernet port and a wireless connection connected simultaneously. If this is always going to be the state of your machine running NTOPNG, then pick whichever NIC you prefer. I used my wired card in the video at the top.

Just make a note of the network interface name for use in our command.

Next we need to create our docker-compose.yml file, or you can copy it from here. Make sure not to copy any extra leading or trailing spaces.

First make a new directory called "ntopng" to work in using the command:

`mkdir ntopng`

then move into that folder with:

`cd ntopng`

Next create the new file in edit mode using:

`nano docker-compose.yml`

Now, type in the following, or copy / paste it in:

```
version: '3'

services:

  ntopng:
    image: vimagick/ntopng
    command: --community -d /var/lib/ntopng -i <your NIC name here> -r 127.0.0.1:6379@0 -w 0.0.0.0:<your preferred host port here>
    volumes:
      - ./data/ntopng:/var/lib/ntopng
    network_mode: host
    restart: unless-stopped

  redis:
    image: redis:alpine
    command: --save 900 1
    ports:
      - "6379:6379"
    volumes:
      - ./data/redis:/data
    restart: unless-stopped
```

In the above file, make sure to change the part that says `<your NIC name here>` to the actual name of the NIC you made note of earlier. Additionally, for the part that says `<your preferred host port here>` enter the port number you prefer to access the interface on (for instance if you want to use 192.168.1.234:21800 - you'd put 21800 for the port number).

Save the file using CTRL+O and then Enter/Return to confirm the save, then CTRL+X to exit nano.

Finally, make a "data" directory for your volume mapping with the command:

`mkdir data`

Now, you're ready to bring up your NTopNG instance with the command:

`docker-compose up -d`

Give it about 1 minute, then visit the machine IP (server IP) of your host and the port number you set in the docker-compose.yml file, and use the default login credentials of

username: admin

password: admin

Once in the application for the first time, you'll be directed to change those values to something you prefer.

If you aren't seeing data updating in the interface dashboard, you might need to re-check your interface name, and ensure you typed it correctly into your docker-compose.yml file. If you have more than one interface card, you may have to try a couple of cards before you find the right one.

I hope you'll find this tool useful, and enjoy using it.

Revision #1
Created 6 April 2023 14:59:09 by Brian McGonagill
Updated 6 April 2023 14:59:57 by Brian McGonagill