nBox - Envision your network with nBox (Embedded Ntop)

Version 1.1
Author: Joseph Guarino – Evolutionary IT
Last edited 05/24/2007

The life of a systems or network administrator requires us to maintain an expansive understanding of our network infrastructure to more effectively manage it. Amidst volumes of complex data that some IT problems present and network management is no exception to these complications. Visual tools allow us to better see trends and make sense of the macro view of our networks. Ntop, nBox, nProbe are just the right FOSS tools that can help us gain greater insight.

What is Ntop/nBox/nProbe

Ntop is an effective libpcap-based GPL application that can serve as a network probe while offering visual web-based insight on your network traffic flows. This was the first of many projects by Ntop founder Luca Deri in 1998. Via rich graphical output and statistical output Ntop helps you to better see how your network is being utilized and in turn it helps us better manage our networks. Ntop is not only easy to set up, configure, and use, but it provides a comprehensive understanding of behind-the-scenes for all time constrained administrators.

nBox and nProbe are also lesser known parts of this amazing FOSS project. nProbe serves as a NetFlow collector or probe that allow you to do advanced network accounting. Netflow is a technology originally created at Cisco in 1996 and is now standardized as Internet Protocol Flow Information eXport (IPFIX/RFC 3917), NetFlow is available from a variety of internetworking vendors and within Nbox/Ntop. Netflow gives you flow monitoring and detailed session level views of network traffic. Another supported standard is sFlow (RFC 3176) which allows you to sample traffic flows and aggregate an holistic understanding of traffic movement. Additionally sFlow is supported with Ntop/nProbe/nBox. nBox is an embedded device that can serve as either or both nProbe and Ntop box as a part of your network monitoring and accounting efforts.

Nbox Features

- **Hardware Support** Any Linux-compatible x86 machine and to 3 10/100/1000 Ethernet interfaces.
- Wide Protocol Support Support for Ipv4/v6, IPX, Netbios, OSI, SCSI, Fibre Channel, etc.
- **Traffic/Protocol Statistics** Graphical breakdown of your network traffic and detailed protocol statistics.
- **Internet Domain AS (Autonomous Systems) and VLAN (Virtual LAN) Statistics** Provides insight into your collection of IP networks and visibility into Layer 2 of the OSI model.
- **NetFlow/sFlow collector support** Offers a birds eye view of session level and network flows with support for industry standard routers/switches.
- **Web-based interface with RDD** As statistical output is most easily comprehensible graphical output, Nbox/Ntop provide this effortlessly.
- **Security Features** - SSL, SSH and firewall. SSL interface for secure access to the web console in a secure manner. Additionally SSH is available for those who crave a CLI as well as a full firewall option.

Its easy to see the benefits in using nBox/nTop to detect, diagnose and address network problems. It presents us with a deeper understanding of application traffic flows, detail trending, and capacity planning.

Hardware/Software Choices

As is customary within the FOSS world, one has a myriad of choices for an actual setup and configuration of applications. Ntop is no exception and you can set it up on a vanilla machine that is Debian GNU/Linux-compatible or build it on a flash-based machine/embedded system which would use nBox. Alternatively, one may purchase a pre-built supported network device from Nmon.net, the commercial wing of Ntop project. In our case, we are going to build an embedded system with nBox.

Install & Setup

In the pile of junk I call my lab as most of us nerds do, I have an old Dell box on which I do all kinds of testing. From the example box I have for building, I have removed the hard drive and replaced it with a 1GB flash device connected to it by a IDE to flash connector.

Note: nBox is available through the Ntop store for 149.95 Euro and at a substantial discount for nonprofits. At this low price you can afford to outfit an entire network with all the benefits of Ntop and additionally Nprobe (Netflows/sFlows) probes at a very low cost. Additionally, this small cost helps support an amazing FOSS project. Given the large price tags on the commercial competitors offerings, this is an extremely cost effective solution.

Prerequisites for Nbox

Machine to be used for nBox that has at least hardware compatibility with Debian GNU/Linux because that is what it is based on.

- Working machine with CF reader or USB CF reader
- Compact Flash of 128mb or greater
- USB Flash Reader
- CF to IDE Adapter

Installing the nBox

Initial setup will require obviously require using a live working system to download the image and then copy it on to your Flash card.

1. Download your purchased nBox code to your local machine.
2. Attach your USB Flash Reader/Writer with CF plugged in it.
3. Run dd to copy firmware to CF -- where 000 is the the name of the device.
4. dd if=cfimage.bin of=/dev/000
5. Now for the open up the box you are going install nBox on and remove the hard drive and screw in your CF to IDE adapter.

6. Attach and screw in your CF to IDE connector so its securely connected and then plug in the nBox CF we just created.
7. Replace the case and reboot.

The default IP of the nBox is 192.168.160.10 so you can connect directly with a network cable from your other machine to this nBox or just hook up your monitor and keyboard. By default you have access to SSH and HTTP access to the device.

Note: Please do change these to strong passwords before you connect this system to any network. Additionally you can consider closing down SSH or adding in additional Iptables in to further restrict access.

SSH -

user = root

password = nbox

Web interface -

user = admin

password = nbox

Placement in the Network

In order to properly capture traffic on your networks you has to be cognizant of probe placement. There are two general ways to capture desired traffic. One is to place the a port in your switching environment into port mirroring mode or SPAN in Cisco-speak. The other is to place a hub on that segment you want to monitor.

Practical Usage

Detecting, diagnosing, and addressing network

problems

Lets say that your management does not understand what is happening to all the available bandwidth on your network and is confounded by the usual generic numbers you provide them. Ntop can be wonderful help in this department by allowing you to offer management a printout of the Ntop >> Summary output. In this way, Ntop can help in addition to your network monitoring/management frameworks.

Understanding application traffic flows

Often performance issues comes to the fore that are not easily transparent. Knowing your traffic flows can help you deal with capacity planning, fixing and even misconfiguration.

Netflows/Sflows

NetFlow and sFlow support allows one a birds-eye-view of whats going on in your network ecosystem. The flexibility, scalability and usability Nbox/Ntop is hard to beat. Given the capital requirements of many of the commercial, closed-source competitors solutions, N-series solutions offer a compelling high-quality and cost-effective alternative.

Commercial Options

The greatest misconception of most in the general IT world is that FOSS has limited or no commercial support. This cannot be further from the truth and with Nbox , the options for the consumer are vast. If you are not inclined to build your own Nbox you can purchase a commercially-supported, easily implemented network device from Luca Deri's company Nmon. Nmon offers commercial support and development for the n* series embedded devices and software for all your networking needs. Nmon corporation offers the strength of these powerful FOSS applications and high quality software/support at a very competitive price point.

- **nCap** wire-speed packet capture and analysis.
- **nProbe** Netflow v5/v9 probe for fast Ethernet or gigabit Ethernet networks.
- **nBox** embedded hardware solution which is a combination of nTop and nProbe in a simple hardware solution.
- **nMirror** embedded hardware for inline traffic analysis.
- **PF_Ring** Kernel based packet capture and sampling that dramatically improves packet capture speeds.

Brain behind the binary and NMON Corporation

I am always interested in the motivating factors behind those who pioneer and forge new technologies in the FOSS world. Recently, I was fortunate enough to spend some time with Luca Deri, and hear his first-hand perspective about these wonderful projects he created. In asking Luca why he created n* projects he aptly replied,

I wanted to solve my network monitoring problems. At that time I was working at the university and they had no tool able to provide a simple answer to common monitoring problem. I decided to release nTop (it was v. 0.3, spring 1998) freely under GPL and the feedback from early users motivated me to go ahead.

The nBox instead is a way to provide users a complete solution for monitoring a remote site and report, by means of NetFlow, traffic information to a central point (e.g. using nTop). I was disappointed that all the available probes were limited or too costly. The nBox is also a way to get some little cash for running the nTop project.

Conclusion

Luca and his team of contributors can rest assured that his goals have been surpassed and they will continue to create innovative networking solutions while remaining committed to FOSS principles. The reputable nBox and various other Nmon solutions are worth a serious consideration for any environment.

Ntop Links

http://www.ntop.org

http://wiki.ntop.org/mediawiki/index.php/

Nmon Solutions

http://www.nmon.net/

http://www.nmon.net/shop/

About Evolutionary IT :::

Joseph Guarino is a Sr. Consultant/Owner at Evolutionary IT which provides systems, network, security, e-marketing, training, project management and FOSS solutions. On his free time you will find him happily building networks, servers and security devices on FOSS, writing on FOSS/security topics or supporting non-profits. Just as often he can be found drumming away in his metal band or laugh hysterically at all sorts of comedy he so constantly enjoys.