

ntopng 安装和基本使用教程

1. 简介	2
2. 版本说明	3
3. 安装 ntopng	3
3.1. 在 ubuntu 18.04 LTS 上安装 ntopng	3
3.2. 在 CentOS 上安装	4
3.3. 启动 ntopng	4
4. Web GUI (ntopng Enterprise L-ubuntu 18.04)	5
4.1. 登录	5
4.2. 仪表盘	5
4.3. 流量报告	6
4.4. 流量	7
4.5. 历史图表	8
4.6. 首选项	10
4.7. 获取 license 并激活	10
5. 在 nprobe 上使用 ntopng 示例	11
5.1. nprobe 简介	11
5.2. 多个 nProbe 到一个 ntopng	
5.3. NAT	13
5.4. 在同一个设备上监视某个接口流量示例	14
6. 在 n2disk 上使用 ntopng 示例	14
6.1. 流量记录简介	14
6.2. 启动流量记录	14
7. ntopng 时间序列和流的磁盘要求	15
8. 购买 license	15
9. 关注我们	15



1. 简介

ntopng 是原始 ntop 的下一代版本, ntop 是监视网络使用情况的网络流量探测器。ntopng 基于 libpcap, 并且以可移植的方式编写,以便实际上可以在每个 Unix 平台, MacOSX 和 Windows 上运行。

ntopng(是的,都是小写字母)提供了直观的,加密的Web用户界面,用于浏览实时和历史流量信息。 主要特点如下:

- 根据多种标准对网络流量进行排序,包括 IP 地址、端口、L7 协议、吞吐量、自治系统(AS)
- 显示实时网络流量和活动主机
- 针对多个网络指标生成长期报告,包括吞吐量和应用协议
- 顶级发言人(发送者/接收者),顶级自治系统,顶级 L7 应用
- 监视并报告实时吞吐量,网络和应用程序延迟,往返时间(RTT),TCP统计信息(重传,乱序数据包,数据包丢失)以及已传输的字节和数据包
- 将持久流量统计数据存储在磁盘上,以便将来进行探索和事后分析
- 在地理地图中对主机进行地理定位和叠加
- 利用 nDPI 和 ntop 深度数据包检测(DPI)技术发现应用程序协议(Facebook, YouTube, BitTorrent等)
- 通过利用 Google 和 HTTP 黑名单提供的特征化服务来表征 HTTP 流量
- 分析 IP 流量并根据源/目的对其进行分类
- 报告 IP 协议使用情况(按协议类型分类)
- 生成 HTML5 / AJAX 网络流量统计信息
- 完全支持 IPv4 和 IPv6
- 完全的第2层支持(包括 ARP 统计信息)
- GTP/GRE 去隧道
- 支持 MySQL, ElasticSearch 和 LogStash 导出监控数据
- 交互式历史浏览的监控数据导出到 MySQL
- 警报引擎以捕获异常和可疑主机
- SNMP v1 / v2c 支持和连续监控 SNMP 设备
- 身份管理,包括 VPN 用户与流量的关联



2. 版本说明

ntopng 软件有四个版本: Community, Professional, Enterprise M, Enterprise L, 每个版本都针对较小的版本解锁附加功能。

ntopng <u>产品页面</u>中提供了功能的完整列表和比较表。

• ntopng Community

社区版本是免费使用的开源软件。完整的源代码可以在 Github 上找到。

• ntopng Professional

专业版提供了一些有关社区的额外功能,这些功能对于中小企业特别有用,包 括图形报告,流量 配置文件和 LDAP 身份验证。

• ntopng Enterprise M

Enterprise M 版本相对于 Professional 版本提供了一些额外的功能,这些功能对于大型组织特别有用,包括 SNMP 支持,快速 MySQL 导出,高级警报管理,高性能流索引。

• ntopng Enterprise L

与 Enterprise M 版本相比, Enterprise L 版本提供了一些额外的功能,包括身份管理(使用户与流量相关联的能力)。此版本还可以解锁 n2disk 1 Gbit(连续记录)和 nProbe Pro(Flow Collection),而无需其他许可证。

3. 安装 ntopng

3.1. 在 ubuntu 18.04 LTS 上安装 ntopng

● 安装 ntop 存储库

sudo apt-get install software-properties-common wget sudo add-apt-repository universe sudo wget http://apt-stable.ntop.org/18.04/all/apt-ntop-stable.deb sudo apt install ./apt-ntop-stable.deb 注(启用 root 权限)

● 安装软件包

sudo apt-get clean all

sudo apt-get update

sudo apt-get install pfring-dkms nprobe ntopng n2disk cento



sudo apt-get install pfring-drivers-zc-dkms

3.2. 在 CentOS 上安装

● 安装库和依赖项

cd /etc/yum.repos.d/

wget http://packages.ntop.org/centos-stable/ntop.repo -O ntop.repo

• CentOS/RedHat 8

rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm

rpm -ivh http://rpms.remirepo.net/enterprise/remi-release-8.rpm

yum install dnf-plugins-core

dnf config-manager --set-enabled PowerTools

dnf config-manager --set-enabled remi

• CentOS/RedHat 7

rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm

• CentOS/RedHat 6

rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm wget https://copr.fedoraproject.org/coprs/saltstack/zeromq4/repo/epel-6/saltstack-zeromq4-epel-6.repo rpm -ivh http://packages.ntop.org/rpm6/extra/hiredis-0.10.1-3.el6.x86_64.rpm

● 安装软件包

yum erase zeromq3

yum clean all

yum update

yum install pfring-dkms n2disk nprobe ntopng cento

如果需要用 PF_RING ZC ,还需安装如下驱动:

yum install pfring-drivers-zc-dkms

3.3. 启动 ntopng

systemctl start ntopng

systemctl status ntopng

<pre>mp@ubuntu:~\$ systemctl start ntopng mp@ubuntu:~\$ systemctl status ntopng ntopng.service - ntopng high-speed web-based traffic monitoring and analysis Loaded: loaded (/etc/systemd/system/ntopng.service; enabled; vendor preset: Active: active (running) since Fri 2020-09-04 02:21:32 PDT; 2s ago Process: 2314 ExecStartPre=/bin/sh -c /bin/sed "/^[]*-e.*\$\\^[]*-G.*\\^[] Process: 2283 ExecStartPre=/bin/sh -c /usr/bin/ntopng-utils-manage-config -a Main PID: 2318 (ntopng) Tasks: 10 (limit: 2295) CGroup: /system.slice/ntopng.service 2318 /usr/local/bin/ntopng /run/ntopng.conf</pre>
Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [NtopPro.cpp:714] [L1 Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:842] Adding Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:851] Adding Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:873] Adding Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [Ntop.cpp:883] Adding Sep 04 02:21:34 ubuntu ntopng[2318]: 04/Sep/2020 02:21:34 [PeriodicActivities.c

4. Web GUI (ntopng Enterprise)

(注意:本教程后续部分均在 ubuntu 18.04 上进行,其他系统使用方法类似)

4.1.登录

启动 ntopng 之后,您可以查看 GUI。默认情况下,可以从任何 Web 浏览器访问 GUI 。在 ntopng 启动期间,可以将其他端口指定为命令行选项。始终弹出的第一页包含登录表单-前提是用户尚未决定在启动过程中关闭身份验证。http://127.0.0.1:3000/,初始账号密码均为: admin,首次登录需重置密码。

● 浏览器打开 web 界面

HongKe

http://127.0.0.1:3000/



4.2. 仪表盘

仪表板是一个动态页面,它为 ntopng 监视的所选接口或接口视图提供当前流量的更新快照。专业版中 www.hkaco.com 广州 深圳 武汉 成都 上海 西安 北京 台湾 香港 400-999-3848

<u>sales@hkaco.com</u> <u>support@hkaco.com</u> 电话:020-38743030, 38743032 传真:020-38743233



的仪表板可提供大量信息,包括实时流量-每个受监视的界面和每个应用程序-本地本地通话者和热门目的 地。仪表板将动态刷新。表格和图表由 ntopng 保持更新。仪表板的右侧部分显示了"主要应用程序和网络 流量"的实时和最新图表。如果选择了网络接口视图,则将按每个物理接口显示网络流量。只需单击图表 键中相应的彩色点,即可动态切换每个图表中显示的项目。

位置: Dashboard->Traffic Dashboard

nens33 * 3.10 kbit/s License expires in 5 Days, 15:33:43	3 20 🔜 9 Devices 36 Flows 🪘		Q Search
Contribute to the project by sending encrypted, anonymous telemetry data	to ntop.org: visit the APreferences page and express your pro-	eference.	
Traffic Dashboard			
ens33: Top Local Talkers	Actual Traffic	ens33: Realtime Top Application Traffic	Network Interfaces: Realtime Traffic
ubuntu [WORKGROUP]	3.37 kbit/s ↑	TI SA Khile.	ern 21 white.
HP LaserJet Professional M1213nf MFP	1.03 kbit/s 🛧	64 Kbits	400 Kbirk
DESKTOP-0H7TMQ9	690.83 bit/s 🛧	48 Kbbb	320 Kbirls
LAPTOP-AC44EIOA	393.39 bit/s 🛧		240 Kbirs
192.168.0.255	393.39 bit/s 🛧	Schools	100 Kbiris
_gateway	254.26 bit/s 🛧	16 Holds	80 Kbirs
ubuntu [IPv6] [ubuntu]	211.09 bit/s 🛧	0 0229-28 0230-23 0231:18 02:32:13 02:33:05	0 02:29:28 02:30:23 02:31:18 02:32:13 02:33:04
ens33: Top Remote Destinations	Actual Traffic	ens33: Top Application Traffic Last Day View	Network Interfaces: Last Day View
224.0.0.251	2.08 kbit/s 个	5.09 Kbitls	1.21 MRHS,
52:36.73.165	1.48 kbit/s ↑	4.8 Kbt/s	1.12 MbHs
239.255.255.250	690.83 bit/s 🛧	4 K005	960 Kbits 800 Kbits
Broadcast	254.26 bit/s 1	2.4 (2005)	640 Kbirls
117.18.237.29	211.09 bit/s 🗸	1.6 Kbets	480 Kbirs
104.123.154.170	211.09 bit/s 🛧	aco bits	160 Kb//s
ff02::fb	211.09 bit/s 1	0232200 063320 120640 174000 231320 0232200	0122200 001120 120640 124000 221220 0

4.3. 流量报告

专业版的 ntopng 允许为受监视的一个或多个接口生成自定义流量报告。可从主工具栏的下拉主菜单访问"Traffic Report"页面,该页面为用户提供了多个配置选项。

左侧有固定宽度的时间间隔。它们分别是 lh (一个小时), ld (一天), lw (一周), lM (一个月), 6M (六个月)和 lY (一年)。单击这些间隔中的任何一个都会生成一个自动报告,该报告的时间范围从 当前开始,并且时间倒退直到达到间隔。







4.4. 流量

可以选择顶部工具栏中的"流"条目,以可视化当前活动流的实时交通信息。可以将流视为两个主机之间的逻辑双向通信通道。同一对主机之间可以存在多个并发流。

nens33	0 bps 403.00 bit/s	License expires	in 5 Days, 15:24:06 16 💭 10 💭 10 Dev	ices 25 Flows 🚍				Q Searc	h	P - 4
Co	ntribute to the project by sendin	g encrypted, ano	nymous telemetry data to ntop.org: vi	sit the APreferences page and expre	ess your preference.					
Activ	e Flows									
Activ	0110003				10 • Hosts •	Status -	Direction - Applica	tions - Catego	ories • IP Version •	Protocol
	Application	Protocol	Client	Server	Duration	Score	Breakdown	Actual Th	ot Total By	tes Info
Into	SSDP 💼	UDP	_gateway 👫:1900	239.255.255.250:1900	20:30		Client	0 bps ·	- 144.01 K	3 —
Info	MDNS 📫	UDP	WORKGROUP	224.0.0.251:mdns	20:43		Client	0 bps ·	- 60.48 K	3 🛧
Info	MDNS 📩	UDP	192.168.0.111 +:mdns	224.0.0.251:mdns	20:43		Client	0 bps ·	- 60.37 K	3 🛧
Info	MDNS 📫	UDP	ubuntu [IPv6] 🍽:mdns	ff02::fb:mdns	20:43		Client	0 bps ·	- 12.54 K	3 🛧
Info	Targus Dataspeed 📩	UDP	_gateway 4:1024	Broadcast:5001	20:40		Client	0 bps ·	- 9.78 K	3 🛧
Info	UPnP 💼	UDP	192.168.0.102 🚓:52893	239.255.255.250:3702	00:15		Client	0 bps ·	- 8.81 K	3 —
Info	? Unknown	UDP	192.168.0.102 🚓:56533	Broadcast:1947	20:12		Client	0 bps ·	- 2.16 K	3 —
Info	? Unknown	UDP	192.168.0.102 🚓:56533	192.168.0.255:1947	20:12		Client	0 bps ·	- 2.16 K	3 —
Info	SSDP 💼	UDP	192.168.0.108 + 54983	239.255.255.250:1900	00:16		Client	0 bps ·	- 1.05 K	3 —
Info	SSDP	UDP	192.168.0.107 👬:50584	239.255.255.250:1900	00:03		Client	0 bps ·	- 864.00 Byte	s —

● IP 搜索



搜索后可以知道特定 ip 的详细信息如下:

■ ens33 • ↓ 182.30 bil/s (Lietuwe express in 5 Days, 252117) [10]	II 🖃 (E Devices) (SE Flows) 🦰	Q Search	A. 1.
Contribute to the project by sending encrypted, anonymous telemetry data to	o ntop.org: visit the $\underline{\mathbb{A}}$ Preferences page and express your preference.		
Host: 192.168.0.113 🚠 🌴 Traffic Packets Ports Peers ICMP Applic	cations DNS TLS SSH HTTP Flows 🛕 🔚 🎦 🌣		
(Router/AccessPoint) MAC Address	Vmware_8D:6B:84 (00:0C:29:8D:6B:84)	Computer 🜻	
IP Address	192.168.0.113 <u>()</u> [192.168.0.0/24]	Host Pool: Not Assigned 0	
os	👌 Linux [Ubuntu]		
Name	WORKGROUP 🗹 🌣 🕼 🖬 Private		
Score Im	0		
db . RTT	13.89 ms		
First / Last Seen	03/09/2020 22:53:47 [03:51:20 ago]	04/09/2020 02:45:05 [00:02 ago]	
Sent vs Received Traffic Breakdown	Sect.	Rod	
Traffic Sent / Received	10,757 Pkts / 1.7 MB 🛧	9,857 Pkts / 6.6 MB	
	As Client	As Server	
Flows: Active / Total / Anomalous / Port Unreach Q	13 4 / 2,079 - / 76 - / 4 -	0 - / 22 - / 9 - / 0 -	
Peers: Active	34	0-	
TCP: Retransmissions / Out of Order / Lost / KeepAlive	Sent	Received	
	301 Pkts - / 11 Pkts - / 37 Pkts - / 233 Pkts -	48 Pkts - / 661 Pkts - / 330 Pkts - / 61 Pkts -	
Reset Host Stats	Reset Host Stats		
Additional Host Names	Source	Name	
	DHCP	ubuntu	
Download 🛓	JSON	1 min 🕑 Fiter (BPF) prog download	



点击 🗯 可查看历史流信息

Host: 192.168.0.113 🚠 🐐 Traffic Packets Ports Peers ICMP Applications DNS TLS SSH HTTP Flows 🛕 🐚 🐲

如下表:



4.5.历史图表

ntopng 可以将流数据转储到持久性存储中,并提供视图以浏览过去记录的流数据。

传统上,为了提供历史数据,ntopng 需要连接的 MySQL 数据库。传统上,为了提供历史数据,ntopng 需要连接的 MySQL 数据库。请查看 Flows Dump 文档,以获取有关如何设置连接的更多详细信息以及此 模式可用的历史视图。

但是,由于用户对 MySQL 的低性能和高流插入率的反馈,ntopng 现在集成了一个称为 nIndex 的专用 流转储数据库,它克服了 MySQL 的限制。当前仅在 Linux / x86 64 体系结构的 ntopng 企业版中可用。

为了将流转储到磁盘, ntopng 要求指定-F nindex 选项。

sudo ntopng -i ens33 -F nindex

位置: interface-> 🕍



广州虹科电子科技有限公司



通过单击该 塑 图标,可以选择特定的通信或主机并分析原始流。

Application	Total Bytes	Percentage		Actions
SSDP	41.0 KB		45.1 %	Q
MDNS	19.99 KB		22.0 %	a
Unknown	11.31 KB		12.4 %	Q
UPnP	9.49 KB	-	10.4 %	Q
DNS	2.51 KB	•	2.8 %	Q
Targus Dataspeed	2.33 KB	•	2.6 %	Q
UbuntuONE	2.07 KB		2.3 %	Q
ICMPV6	1.06 KB	•	1.2 %	Q
IGMP	917.0 Bytes	•	1.0 %	Q
NetBIOS	245.08 Bytes		0.3 %	Q

NOTES:

ī.

点击后,何以看到每个用户的使用情况

n ens33 • \$ 3.30 kbit/	License expires in 5 Days, 15:08:47	7 🔲 8 Devices 25 Flows 🚍			Q Search		₽-
Interface: ens33 🕋 Networks	Packets Applications ICMP ARP						
		Begin Date/Time:	End Date/Time:				
5m 30m 1h 1d 1w	1M 1Y Custom	04/09/2020 02:51:00	64/09/2020 02:	57:00 🗰 Apply	$\leftrightarrow \rightarrow + -$	8 🖿	
SSDP -							
1.16 Kbit/s 1.12 Kbit/s					SSDP OTrend OEMA OSMA	O Awg O 96th Perc	
960 bit/s							
800 bit/s							
640 bit/s							
480 bit/s							
320 bits							
0							
02:51:00	02.52.00	02:53:00	02:54:00	02 55.00	02:56:00	02	2:57:00
Total: 48.71 KB	951	h Percentile: 1.16 Kbit/s	Average: 1.11 Kbit/s	Mac 1.16	Kbit/s @ 04/09/2020 02:52:00		
Top SSDP L7 Contacts • X Appl	ication: SSDP				10	IP Version •	Explore
Client		Server		Throughput		Total Bytes	Action
_gateway		239.255.255.250		780.22 bit/s		34.29 KB	Q
192.168.0.102		239.255.255.250		95.56 bit/s		4.2 KB	Q
192.168.0.107		239.255.255.250		57.6 bit/s		2.53 KB	Q

再次点击 🔍 图标可以看到特定用户的流量使用情况:



广州虹科电子科技有限公司

▲ ens33 -	e expires in 2 Days, 19:11:11 12 💷 6 💷 (8 Devices (13 Flows)		Q	. Search	₽ -
Host: 192.168.0.113 🚠 Traffic Packet	s Ports Peers ICMP Applications DNS TLS SSH HTTP Flows 🛕	医 首 章			
_	Begin Date/Time:	End Date/Time:			
5m 30m 1h 1d 1w 1M 1Y	05/09/2020 22:55:00	6/09/2020 22:55:00	Apply ← → +	- 🕜 🖿	°
Top Applications *					
5.59 Kbit/s		fntop TLS DNS Am	IZCN HTTP MDNS OUbuntuONE OUnknown Oother	Trend OEMA SMA OAvg	
4.8 Kbb/s					
4 Kbit/s					
3.2 Kbit/s					
2.4 Kbi/s					
1.6 Kbit/s					
800 bit/s					
0 22:55 00:55	02.55 04:55 06:55 08:55	10.55 12.55 14.50	16:55 18:55	20.55 2	2.55
Total: 1 20 MB	Average: 125.05 hitle		May: 5.59 Kitele @ 05/09/2020 20:55:00		
Top 17 Contacts -	Protogo, Alcone mar		max. 5.55 mars @ 60/051202 10:5000		-
Client	Sanar	Application	Throughout	Total Butor	Acti
WORKGROUP	125.74.34.246	нтр	544.94 bit/s	5.61 MB	ACO
WORKGROUP	nton-digitalosean.ntop.org	ntop	307.23 bit/s	3.16 MB	0
WORKGROUP	118.116.2.26	TLS	135.18 bit/s	1.39 MB	e

4.6.首选项

在 Setings->Preferences 中可以配置 ntopng,例如我们可以设置时间序列的分辨率,

€ ens33 • ↓ 100 40	2.00 bit/s License expires in 2 Days, 19:21:32 15 🖬 11 🖬 9 Devices 27 Flows	Q Search
Runtime Prefe	rences	
A Search Preferences	Timeseries Database	
User Authentication	Timeseries Driver The driver used for storing and retrieving timeseries data.	RRD
Network Interfaces	InfluxDB URL	http://localhost:8086
Cache Settings	The UKL pointing to a running imuxus instance.	
Timeseries	InfluxDB Database	ntoona
Alerts	The database to use for timeseries storage. Existing data will not be migrated.	
Alert Endpoints	InfluxDB Authentication	
Applications	Enable InfluxDB authentication.	
Logging	Timeseries Resolution The interval between consecutive timeseries data points for local bosts. Only effective for	10s <mark>30s</mark> 1m 5r
Flow Database Dump	packet interfaces.	
SNMP	 High resolution can have a strong impact on memory and disk usage for large networks. 	
Network Discovery	Timeseries retention time can be set here	
Telemetry	Interfaces Timeseries	
Traffic Recording	Traffic Toole the creation of bytes and packets timeseries.	

4.7. 获取 license 并激活

在 Help->About 查看软件版本获取 License, 点击图中所示位置。



广州虹科电子科技有限公司

n	■ ens33 • 1.30 kbit/s 1.70 kbit/s 1.70 kbit/s 1.70 kbit/s	Sa Flows	Q Search	R- 1
Dashboard	Contribute to the project by sending encrypted, anonymous telemetry data to ntop.org:	visit the APreferences page and express your preference.		
Alerts	About ntopng			
Flows	Copyright	© 1998-20 - ntop.org 点击		
Hosts Interface	License	EULA [Systemic] 380071800000001112] Gula on balance use of provider part production was accurate trans, or parchase hanno at 6 often, Il you are no-profit, research or an education antibulou please real Bits. Lonsons: EB8404510EFC000AA8E3E2DB0F207815199999971F4E8A039		
Settings	Version	4.0.200828 (11284) - Enterprise L Edition		
	Built on	Ubuntu 18.04.5 LTS		
Developer	Platform	Debian buster/sid [x86_64][Ubuntu 18.04.5 LTS] - 64 bit		
ee '	Startup Line	ntopngdump-flows "[hidden]"		
	nDPI	3.2.0-2220-6735bb35		
	cURL	7.58.0		
	Twitter Bootstrap	4.4.0		
	Font Awesome	5.11.2		
	RRDtool	1.7.0		
	nindex	1.2		
	Timeseries Resolution	5m		
	Redis Server	4.0.9		
	Mongoose web server	3.7		

点击后会跳转到生成 license 生成界面:

Required Information		Description You can exist
System Id:	3B90718600860F11	Tou can print this informati on within nio pag. Go to m enu Home / A bout and you will find a UR I to thick on. J It do thinks page with a II the Research g information pre-filled. Example. IF F710B8-0882 -5C67-7105A 182
Order Id:		This is the 10 digit orderId you have place ed when shoppe d on the ntop site. Example: 129 883843
Email:		This is the e mal associate d with the or dor id. Example: me @company.co m
ntopng Version:	4.0.200828	Example: 2.0. 150530
ntopng Edition:	Enterprise L (x64)	ntopng editio n type,
• The Enterprise L out license.	dition, creates a single license that also unlocks n2disk and nProbe. This means that with a single meanse you car	unlock all products without the need to generate an individual prod
	Create atoppo License Reset	

在上图中输入购买 license 得到的 Order id 和 Email 再点击 Creat ntopng License 即可生成 License,依据生成 License 后界面提示信息即可完成激活。

5. 在 nprobe 上使用 ntopng 示例

5.1. nprobe 简介

ntopng 可用于可视化 nProbe 生成或收集的交通数据。在几种情况下,将 ntopng 与 nProbe 一起使用很 www.hkaco.com 广州 深圳 武汉 成都 上海 西安 北京 台湾 香港 400-999-3848



方便,包括:

通常由路由器,交换机和网络设备产生的 NetFlow / sFlow 数据的可视化。在这种情况下,nProbe 从设备收集并解析 NetFlow / sFlow 流量,并将结果流发送到 ntopng 以进行可视化。

监视连接到远程系统的物理网络接口。在这种情况下,ntopng无法直接监视网络接口,也无法看到其数据包。一个或多个 nProbe 可用于捕获远程网络接口流量并将结果流发送到中央 ntopng,以进行分析和可视化。

下图总结了上面突出显示的两种情况,并说明了它们也可以组合在一起。



5.2. 多个 nProbe 到一个 ntopng

使用单个 ntopng 从多个 nProbe 收集流对于单个位置负责可视化和存档流量数据很有用。



要从多个 nProbe 收集流, ntopng 必须以额外的开始 C(为收集器)在 ZMQ 端点的末尾, 而每个 nProbe 都需要选择--zmq-probe-mode。在这种配置中, nProbes 会启动与充当服务器的 ntopng 的连接, 反之亦然。因此, 您必须确保 ntopng 正在侦听 ANY 地址(即通配符)*在 ZMQ 端点地址中)或在各种 nProbe 可以访问的另一个地址上。

以下是这种配置的示例

 www.hkaco.com
 广州|深圳|武汉|成都|上海|西安|北京|台湾|香港
 400-999-3848

 sales@hkaco.com
 support@hkaco.com
 电话:020-38743030, 38743032
 传真:020-38743233



ntopng -i tcp://*:5556c

nprobe --zmq "tcp://<ip address of ntopng>:5556" --zmq-probe-mode -i eth1 -n none -T "@NTOPNG@" nprobe --zmq "tcp://<ip address of ntopng>:5556" --zmq-probe-mode -i none -n none --collector-port 2055 -T "@NTOPNG@" nprobe --zmq "tcp://<ip address of ntopng>:5556" --zmq-probe-mode -i none -n none --collector-port 6343 -T "@NTOPNG@"

5. 3. NAT

nProbe 和 ntopng 的 IP 可达性不能总是被认为是理所当然的。有时, ntopng 可能有必要从单独网络中的 nProbe 收集流,该网络可能位于 NAT 之后,甚至被防火墙屏蔽。同样, NAT 后的 ntopng 可能有必要从 另一个网络中的 nProbe 收集流。幸运的是,要处理这些情况,可以将 ntopng (和 nProbe)配置为可互换 地充当 JSON-Over-ZMQ 通信的客户端或服务器。这样就避免了在网络设备中插入冗长,耗时且可能不安 全的规则,因为这足以确保客户端可以访问服务器,而 NAT 将自动处理通信中返回的服务器到客户端部 分。

当 nProbe 和 ntopng 都在同一网络上,或者当 ntopng 在另一个网络中但可以到达 nProbe 时,应使用以下配置





5.4. 在同一个设备上监视某个接口流量示例

配置 ntopng:

sudo ntopng -i tcp://127.0.0.1:5556

配置 nprobe:

sudo nprobe --zmq "tcp://*:5556" -i ens33 -n none -T "@NTOPNG@"

配置完成后即可打开 web 界面:

mp@ubuntu: ~		mp@ubuntu: ~	000
File Edit View Search Terminal Help		File Edit View Search Terminal Help	
06/Sep/2020 23:13:18 [NtopPro.cpp:703] [LICENSE] License:	rYNf7YwLUveBnG/F	SITE'. Discarded.	
QKg09pGyQBkG936vfxpssNKS/XXU/11tIUKJ9Amp0xPbWH5QSt9cK		06/Sep/2020 23:13:54 [template.c:2631] WARNING: Unable to locate template	'DNS_Q
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE]	sq9A+sremi4+R4L0	UERY'. Discarded.	
xJ1cGiKqBhn9ADqgJ2Eh4FyjhlyXQJGZzABIKbU6xB43GdCWMSMPJ		06/Sep/2020 23:13:54 [template.c:2631] WARNING: Unable to locate template	'HTTP_
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE]	NFDfbuScqj8j0yqS	URL'. Discarded.	
brd13u8Vqd0tPJ5M0SJZW2YD8JfJKoWA/06KHtC80paE8kBlDfRjj		06/Sep/2020 23:13:54 [template.c:2631] WARNING: Unable to locate template	'HTTP_
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE]	MXp+U25qhab01KrF	SITE'. Discarded.	
y4VT3g9HrjD8ORC1WmgfEONTpYYPVtlfbjtISNJ+JnHKwYbltWRgH		06/Sep/2020 23:13:54 [plugin.c:1309] 0 plugin(s) enabled	
06/Sep/2020 23:13:18 [NtopPro.cpp:704] [LICENSE]	PA0VkaHQwYK/3jl6	06/Sep/2020 23:13:54 [nprobe.c:9142] Each flow is 208 bytes long	
j9/iKKrpZ3uWve/PlFTu9YtdbIEOGuLs+vHPcS3g0K/TczdFRg==		06/Sep/2020 23:13:54 [nprobe.c:9143] The # flows per packet has been set to	0 6
06/Sep/2020 23:13:18 [NtopPro.cpp:708] [LICENSE] License Hash:	E9B4964310E5FC00	06/Sep/2020 23:13:54 [nprobe.c:9146] IP TOS is ignored	
DAA8E3E2DB0F267B1599699971F4E8A039		06/	vice e
06/Sep/2020 23:13:18 [NtopPro.cpp:714] [LICENSE] Validity:	Until Wed Sep 9	ns33	
18:06:11 2020		06/Sep/2020 23:13:54 [pro/pf_ring.c:424] Dumping traffic statistics on /pro	oc/net
06/Sep/2020 23:13:18 [PeriodicActivities.cpp:105] Started perio	dic activities lo	/pt_ring/stats/7813-ens33.6	
op		06/Sep/2020 23:13:54 [pro/pf_ring.c:496] PF_RING enabled on ens33	
06/Sep/2020 23:13:35 [startup.lua:214] Startup completed		06/Sep/2020 23:13:54 [nprobe.c:9990] Flows ASs will not be computed (no Ge	oDB fi
06/Sep/2020 23:13:35 [PeriodicActivities.cpp:165] Each periodic	activity script	Les Loaded)	
will use 2 threads		06/Sep/2020 23:13:54 [util.c:5029] Initializing ZMQ as server	
06/Sep/2020 23:13:35 [NetworkInterface.cpp:2352] Started packet	polling on inter	06/Sep/2020 23:13:54 [util.c:5108] Succesfully created ZMQ endpoint tcp://	*:5556
Tace tcp://127.0.0.1:5556 [td: 3]	100 M	06/Sep/2020 23:13:54 [util.c:4078] nProbe changed user to 'nprobe'	
06/Sep/2020 23:13:35 [2MQCollectorInterface.cpp:255] Collecting	TLOWS ON tcp://1	06/Sep/2020 23:13:54 [export.c:548] Using TLV as serialization format	
□		06/Sep/2020 23:13:54 [nprobe.C:10361] nProbe started successfully	

打开 Web GUI 界面以后可以看见此时的接口变为 tcp://127.0.0.1:5556

m ICp://127.0.0.1:5556 * 12.40 KDIVS License expires in 2 Days, 18:49:40 34 9 Devices 41 Flows	▲ tcp://127.0.0.1:5556 ▼	12.40 kbit/s	License expires in 2 Days, 18:49:40	34 🔲 9 Devices 41 Flows
--	--------------------------	--------------	-------------------------------------	-------------------------

6. 在 n2disk 上使用 ntopng 示例

6.1. 流量记录简介

当需要解决网络问题或分析安全事件时,及时回溯并深入到数据包级别对于找到导致问题的确切网络 活动至关重要。连续流量记录提供了进入网络历史记录的窗口,使您可以检索和分析该时间段内的所有原 始流量。

注意:

ntopng Enterprise L 已经包含一个 n2disk 1 Gbit 许可证,如果安装了 ntopng Enterprise L 许可证,则无 需购买 n2disk 许可证。

6.2. 启动流量记录

为了实际开始记录流量,您需要从"Interface"菜单中选择一个接口,单击 🚍 图标,然后配置记录实



例:

1. 选择"Traffic Recording"

2. 配置所需的"Max Disk Space"值。这使您可以控制用于 pcap 文件的最大磁盘空间,这也会影响数据保留时间(超过最大磁盘空间时,最早的 pcap 文件将被覆盖)。请注意,数据保留时间还取决于被监视网络的流量吞吐量。

3. 按"Save Setting"按钮实际开始记录。

n	■ lo • ↓ 196.60 kbit/s License expires in 2 D	ays, 15:36:30 3 🔲 1 🖳 (61 Flows)	Q Search	P - <u>+</u> -			
Dashboard	Contribute to the project by sending encrypted, anonymous telemetry data to ntop.org: visit the <u>APreferences</u> page and express your preference.						
Alerts	Interface: Io 😤 Networks Packets Applications ICMP 🔟 💼 🛦 皆 🌣 🌽 🎖 😩 🖣						
Flows Hosts	External traffic recording providers detected, ntopng can automatically bind this interface to an external provider. You can let ntopng take care of the recording using this page, or you can 🌣 configure 🗙 an external traffic recording provider.						
interface	✿ Settings						
Settings	Thatfic Recording Settings						
	Traffic Recording	Continuous Traffic Recording					
Developer	Max Disk Space	2 GB Maximum disk space used for recorded traffic on disk. 0.02 GB are already in use by this instance.					
Thesp	Storage Directory	/var/lib/ntopng/1/pcap					
	Storage Utilization	System (8.95 GB) Packet Dumps (18.1 MB) Extracted Packets (0 Bytes) Free (10.59 GB) - Total: 19.56 GB					
	NOTES: • Global settings (e.g. the license key) can be configure	ed from the Traffic Recording preferences.	Save 5	Settings			

7. ntopng 时间序列和流的磁盘要求

详解计算网址:

https://www.ntop.org/ntopng/ntopng-disk-requirements-for-timeseries-and-flows/

8. 购买 license

可在如下网址联系我们购买:

https://hongwangle.com/ntop/traffic-analysis-and-enforcement/

9. 关注我们

想了解跟多信息,可扫描下方二维码关注&联系我们。



HongKe 虹科

网络安全与可视化

网络可视化,网络监控,时间服务器



400-999-3848

≥ support@hkaco.com

hongwangle.com

广东省广州市高新技术产业开发区科
 学大道99号科汇金谷三街2号701室