

ntopng 应用示例

广州虹科电子科技有限公司
www.hocyber.com

扫描关注



ntopng 应用示例

No.	应用示例	描述	跳转
1	实时流分析	<ul style="list-style-type: none">实时展示接口的Flow（会话）统计信息。	点击这里
2	主机流量详细分析	<ul style="list-style-type: none">实时/回溯分析特定主机流量详细使用情况。	点击这里
3	接口流量详细分析	<ul style="list-style-type: none">实时/回溯分析特定接口流量详细使用情况。	点击这里
4	历史流回溯分析	<ul style="list-style-type: none">回溯分析特定定接口或主机的历史Flow, 应用信息。	点击这里
5	实时抓包分析	<ul style="list-style-type: none">从指定接口实时抓取流量保存为PCAP文件进行详细分析。	点击这里

ntopng 应用示例

No.	应用示例	描述	跳转
6	全流量回溯分析	<ul style="list-style-type: none">• ntop提供全流量存储回溯分析的功能。	点击这里
7	SNMP监控	<ul style="list-style-type: none">• 使用SNMP监控网络设备接口状态和流量。	点击这里
8	主机池划分	<ul style="list-style-type: none">• 根据IP、网段、MAC划分逻辑主机池单独生成流量统计信息。	点击这里
9	活动监控	<ul style="list-style-type: none">• 监控特定主机可达性或者主机服务可用性或者测试网络带宽。	点击这里

ntopng 应用示例

实时流分析

[\[返回主页\]](#)

ntopng 应用示例

● 实时流分析:Flow

可以选择左侧工具栏中的“Flows”条目来可视化当前活动流量的实时流量信息。可自定义排序方式和过滤显示。

1 选择接口

2 过滤, 排序

Application	Protocol	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
SFlow	UDP	192.168.2.1 :44374	devel :6343	19:47	25	Client	16.42 kbit/s ↓	6.42 MB	
ICMP	ICMP	devel	192.168.2.1	19:47	20	Client	4.72 kbit/s ↑	626.3 KB	Port Unreachable
NetFlow	UDP	192.168.2.144 :2055	devel :2056	19:48	25	Client	3.33 kbit/s ↑	1.31 MB	
DHCP	UDP	NolP:bootpc	Broadcast:bootps	19:47	0	Client	1.09 kbit/s ↑	128.58 KB	
SSDP	UDP	192.168.2.136 :3903	239.255.255.250:1900	00:30	0	Client	278.38 bit/s ↓	1.17 KB	
ICMP	ICMP	devel	192.168.2.1	00:04	0	Client Server	0 bit/s —	980 Bytes	Echo Reply
ICMP	ICMP	devel	192.168.2.1	00:04	0	Client Server	0 bit/s —	980 Bytes	Echo Reply
ICMP	ICMP	devel5	devel	19:48	20	Client	0 bit/s ↓	219.97 KB	Port Unreachable

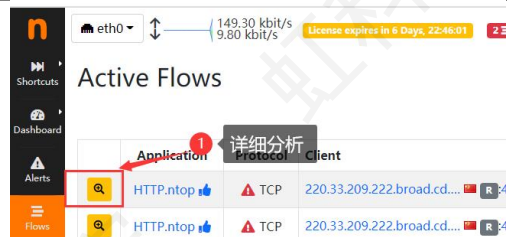
活动流页面

[\[返回主页\]](#)

ntopng 应用示例

● 实时流分析:Flow

点击  可以详细分析某个流。



Flow: 220.33.209.222.broad.cd...:44233 ⇄ izwz9bhxg6t9vtmz3oggz3z:3000 Overview	
Flow Peers [Client / Server]	220.33.209.222.broad.cd... R :44233 [EE:FF:FF:FF:FF:FF] ⇄ izwz9bhxg6t9vtmz3oggz3z:3000 [00:16:3E:08:83:95]
Protocol / Application	TCP / HTTP.ntop (Web) 🍌
First / Last Seen	09/07/2021 10:54:50 [00:04 sec ago] 09/07/2021 10:54:51 [00:03 sec ago]
Total Traffic	Total: 73.45 KB Goodput: 68.67 KB (93.49 %)
	Client → Server: 29 Pkts / 2.48 KB Client ← Server: 55 Pkts / 70.97 KB
DSCP / ECN [Client / Server]	Unknown [5] / Disabled (0) Best Effort [CS0] / Disabled (0)
RTT Time Breakdown	21.58 ms (client)
Client/Server Estimated Distance	4,338 Km 2,691 Miles
Application Latency	226.89 ms
Packet Inter-Arrival Time [Min / Avg / Max]	Client → Server: < 1 ms / 16.37 ms / 265 ms Client ← Server: < 1 ms / 8.21 ms / 226 ms
TCP Packet Analysis	Client → Server / Client ← Server
Out of Order	0 Pkts / 2 Pkts
Lost	0 Pkts / 1 Pkt
Max (Estimated) TCP Throughput	Client → Server: 88.15 kbit/s Client ← Server: 191.12 kbit/s
TCP Flags	Client → Server: S A F P Client ← Server: S A F P

[\[返回主页\]](#)

ntopng 应用示例

主机流量详细分析

[\[返回主页\]](#)

ntopng 应用示例

● 主机流量分析:Hosts->Hosts

此页面显示了所有监视网络接口的主机实时流量统计。可以单击列标题以降序（升序）顺序对结果进行排序。表格右上角提供了其他排序选项。点击主机可查看特定主机详细统计信息。

The screenshot shows the ntopng interface for the 'Hosts' section. At the top, there's a search bar and a 'Search' button (labeled '搜索' with a red '2'). Below the search bar, there are sorting options: '10' items per page, 'IP Version', 'Direction', and 'Filter Hosts'. A 'Filter' button (labeled '过滤' with a red '1') is also present. The main table lists various hosts with columns for IP Address, Location, Flows, Total Bytes Sent, Name, Seen Since, Breakdown, Throughput, and Total Bytes. The table is sorted by Total Bytes Sent in descending order.

	IP Address	Location	Flows	Total Bytes Sent	Name	Seen Since	Breakdown	Throughput	Total Bytes
Flows	192.168.2.222	Local	32	58.47 MB	devel	03:22:05	Sent Rcvd	93.91 kbit/s ↓	167.67 MB
Flows	192.168.2.221	Local	23	6.22 MB	ubun	03:22:05	Sent Rcvd	53.28 kbit/s ↓	47.01 MB
Flows	192.168.2.1	Local	5	46.32 MB	192.168.2.1	03:22:04	Sent Rcvd	32.77 kbit/s ↓	53.04 MB
Flows	192.168.2.225	Local	2	2.3 MB	develv5	03:22:04	Sent Rcvd	3.5 kbit/s ↓	7.35 MB
Flows	192.168.2.144	Local	1	53.19 MB	192.168.2.144	03:22:05	Sent	2.22 kbit/s ↓	53.19 MB
Flows	192.168.6.7	Remote	1	0	192.168.6.7	12:34	Rcvd	2.14 kbit/s ↓	399.53 KB
Flows	0.0.0.0	Broadcast	1	81.16 KB	NoIP	12:33	Sent	1.09 kbit/s ↑	81.16 KB
Flows	255.255.255.255	Broadcast	1	0	Broadcast	12:33	Rcvd	1.09 kbit/s ↑	81.16 KB
Flows	192.168.2.136	Local	2	199.32 KB	192.168.2.136	03:22:01	Sent	228.74 bit/s ↓	199.32 KB
Flows	239.255.255.250	Multicast	2	0	239.255.255.250	00:50	Rcvd	228.74 bit/s ↓	2.57 KB

Showing 1 to 10 of 21 rows. Idle hosts not listed.

[\[返回主页\]](#)

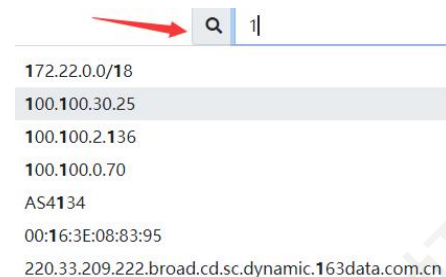
ntopng 应用示例

● 进入主机详情页面: 

在Flow, Host->Host或者其他位置搜索栏搜索IP地址可跳转到主机详情页面, 或者在任意界面点击感兴趣的IP也能进行跳转。

搜索框提供了一种方便的方式来搜索 ntopng 中的许多流量元素:

- Mac主机 (按地址和名称)
- IP地址
- 自治系统
- 动态SNMP 设备



[\[返回主页\]](#)

ntopng 应用示例

● 主机详情:

222.209.33.220

Search Host

通过上文方法进入主机详细页面后顶部菜单提供了许多选项，可以查看分析指定IP详细历史流量信息，包括应用程序，HTTP，TLS统计，历史流详细等等。

Host: 192.168.2.222 Traffic Packets Ports Peers ICMP Applications DNS TLS SSH HTTP Flows

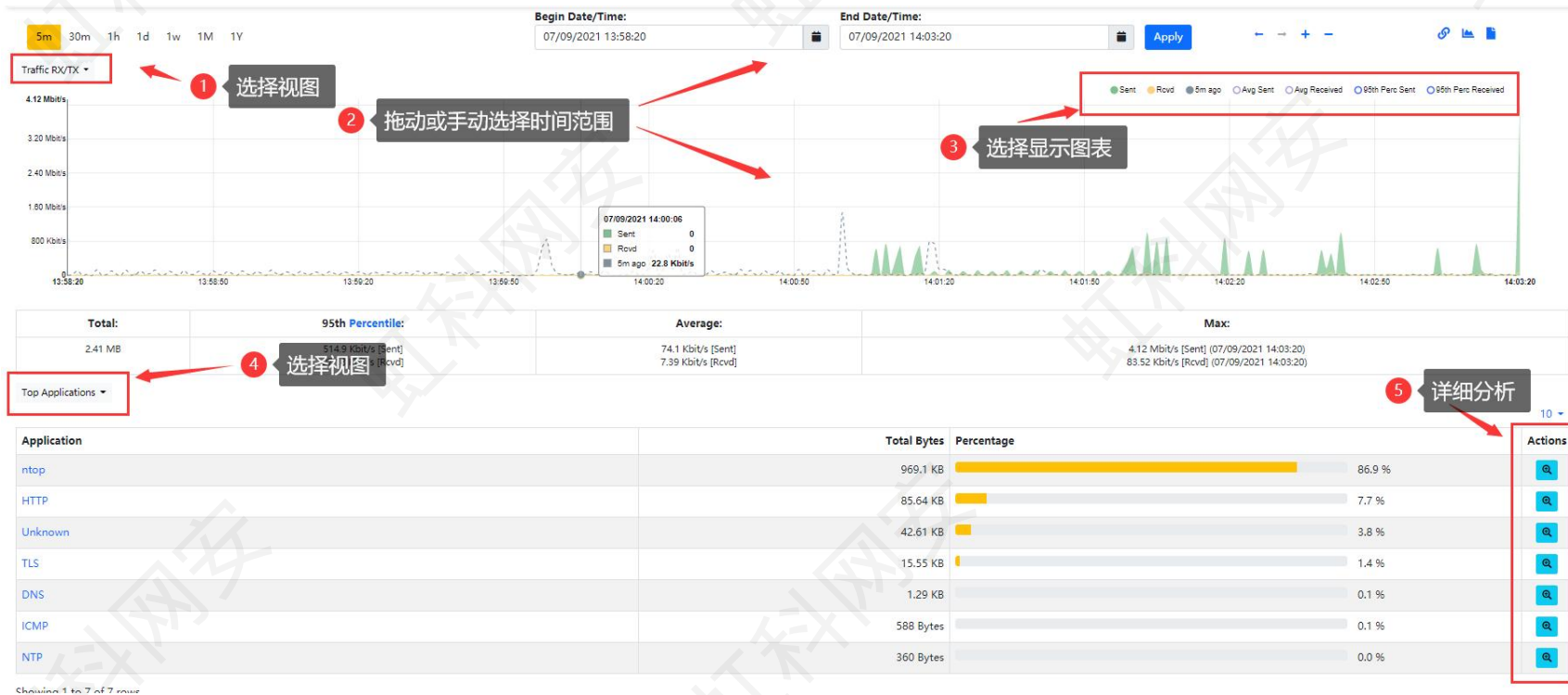
(Router/AccessPoint) MAC Address	SuperMic_D4:CC:F9 (00:25:90:D4:CC:F9)	Router/Switch
IP Address	192.168.2.222 [192.168.2.0/24]	Host Pool: office
Name	devel Local Private	
Engaged Alerts	1	
Score	110	
RTT	Add RTT	
Active Alerted Flows	6	
First / Last Seen	02/04/2020 11:41:44 [03:35:52 ago]	02/04/2020 15:17:35 [00:01 ago]
Sent vs Received Traffic Breakdown		
Traffic Sent / Received	103,793 Pkts / 63.9 MB ↑	398,033 Pkts / 114.7 MB ↑
	As Client	As Server
Flows: Active / Total / Anomalous / Port Unreach	6 - / 882 - / 0 - / 4 -	14 - / 16,623 ↑ / 149 - / 4 -
Peers: Active	3 -	4 -
TCP: Retransmissions / Out of Order / Lost / KeepAlive	Sent 65 Pkts - / 2 Pkts - / 4 Pkts - / 0 Pkts -	Received 107 Pkts - / 27 Pkts - / 13 Pkts - / 0 Pkts -
Reset Host Stats	Reset Host Stats	
Additional Host Names	Source	Name
	DHCP	devel
Download	JSON	1 min Filter (BPF) pcap download

[\[返回主页\]](#)

ntopng 应用示例

● 主机历史流：主机详细页面->

历史流统计页面提供所选主机的历史流量统计信息。用户可以选择基于协议过滤统计数据并以多种格式（例如，字节、数据包、流等）显示数据。
（需启用历史流存储功能 $-F=nindex$ ）



[\[返回主页\]](#)

ntopng 应用示例

接口流量详细分析

[\[返回主页\]](#)

ntopng 应用示例

● 接口:

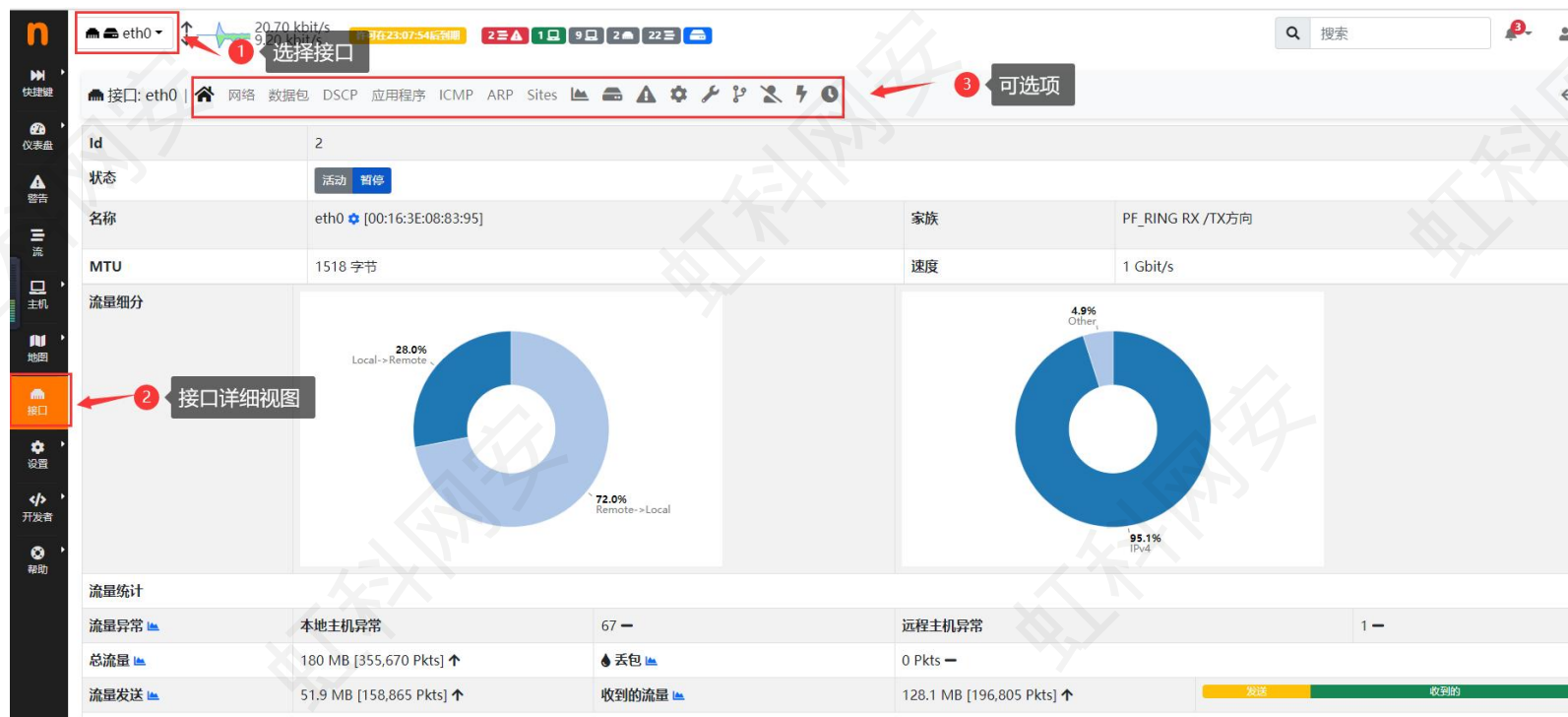
顶部工具栏中的 *Interfaces* 下拉菜单条目包含列出当前由 *ntopng* 监控的所有接口。*ntopng* 中始终存在一个特殊接口，即 [System Interface](#)。*ntopng web GUI* 中显示的大部分数据和信息都与当前选择的接口有关。只需单击其名称即可选择列出的任何接口。



ntopng 应用示例

● 接口详细: Interface

单击 *Interface* 查看当前选择的接口的流量统计信息，顶部菜单提供了许多可选项，包括数据包统计，应用程序统计，历史流量视图，历史警告等等。

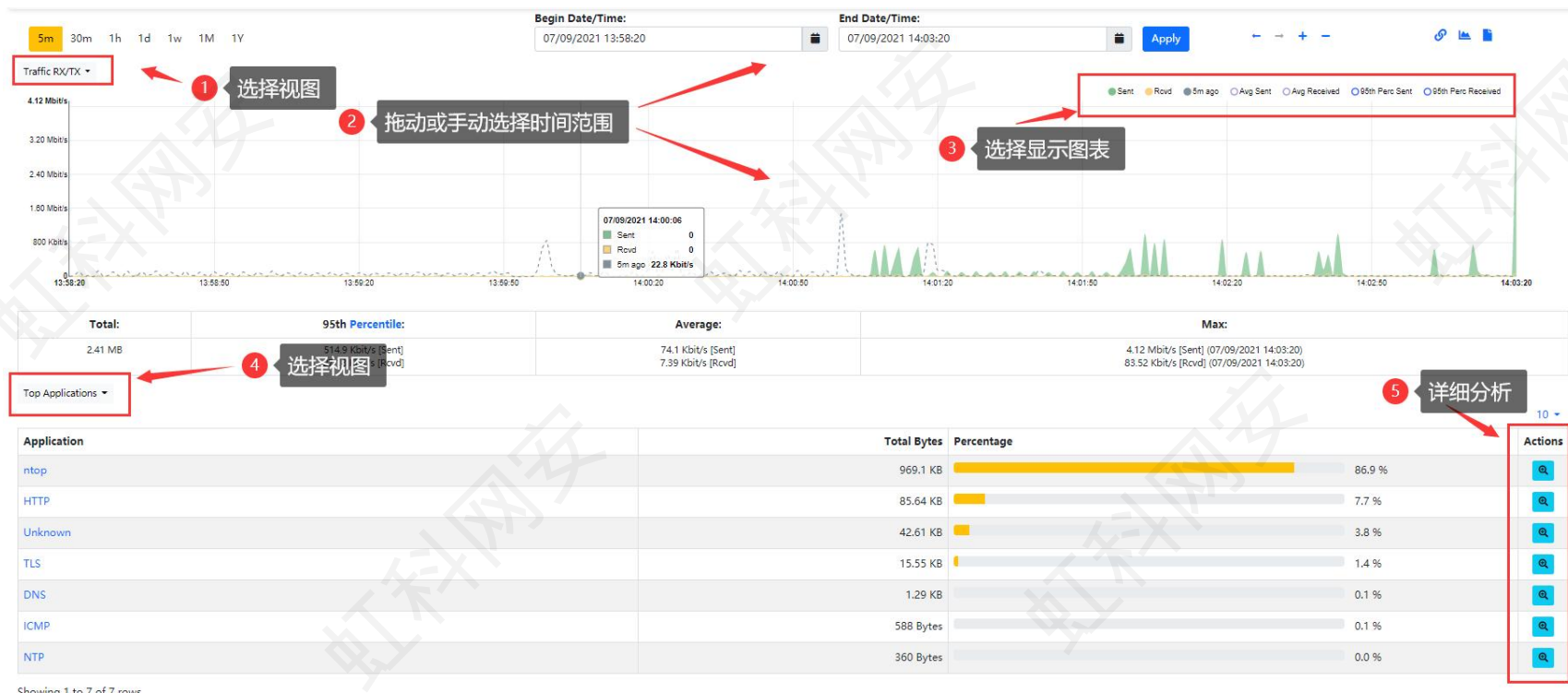


[\[返回主页\]](#)

ntopng 应用示例

● 接口历史流量视图: Interface->

统计页面提供所选接口的历史流量统计信息。用户可以选择基于协议过滤统计数据并以多种格式（例如，字节、数据包、流等）显示数据。



[\[返回主页\]](#)

ntopng 应用示例

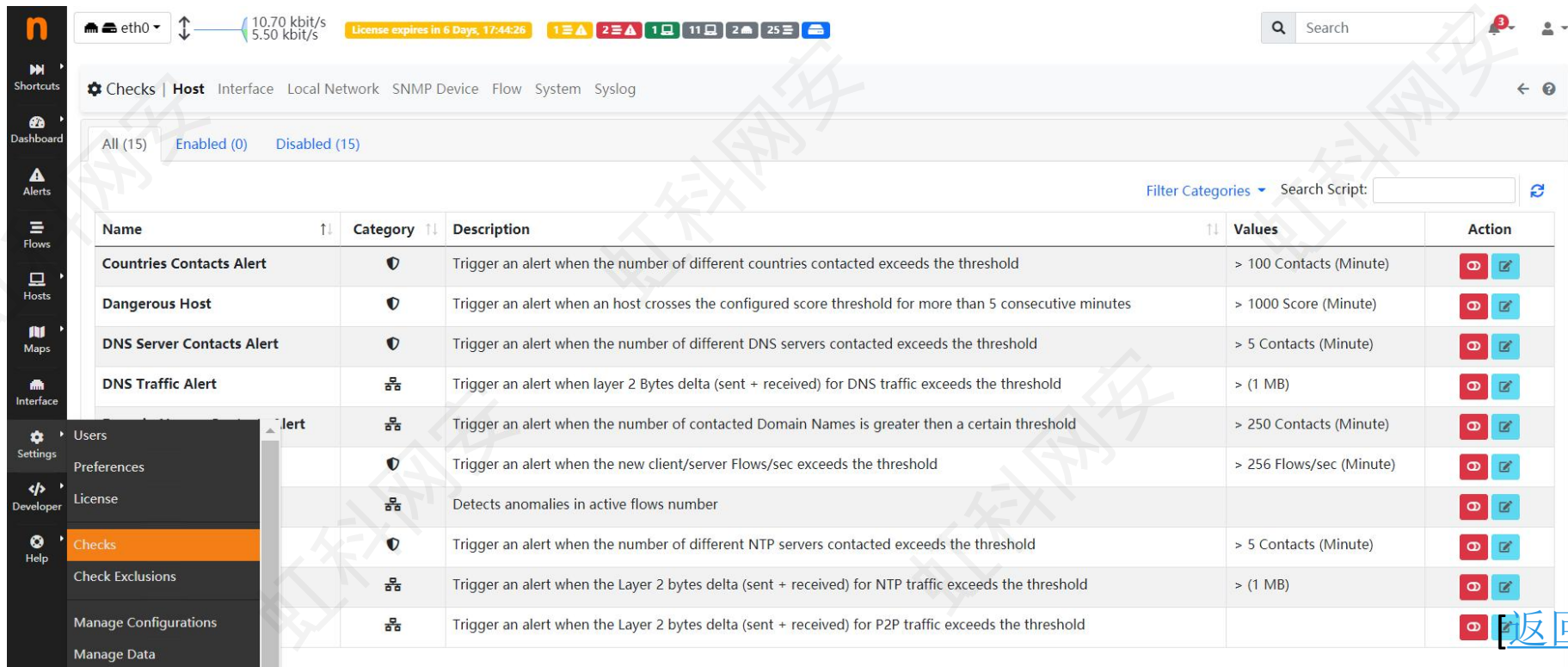
警告

[\[返回主页\]](#)

ntopng 应用示例

● 警报设置: Setting->Checks

ntopng 警报使用 [Checks](#) 进行评估。对主机、接口、SNMP 设备和其他网络元素执行检查，并可通过设置进行配置。



The screenshot shows the ntopng web interface for configuring checks. The 'Checks' menu is open, highlighting the 'Checks' option. The main table lists various checks with their categories, descriptions, values, and actions.

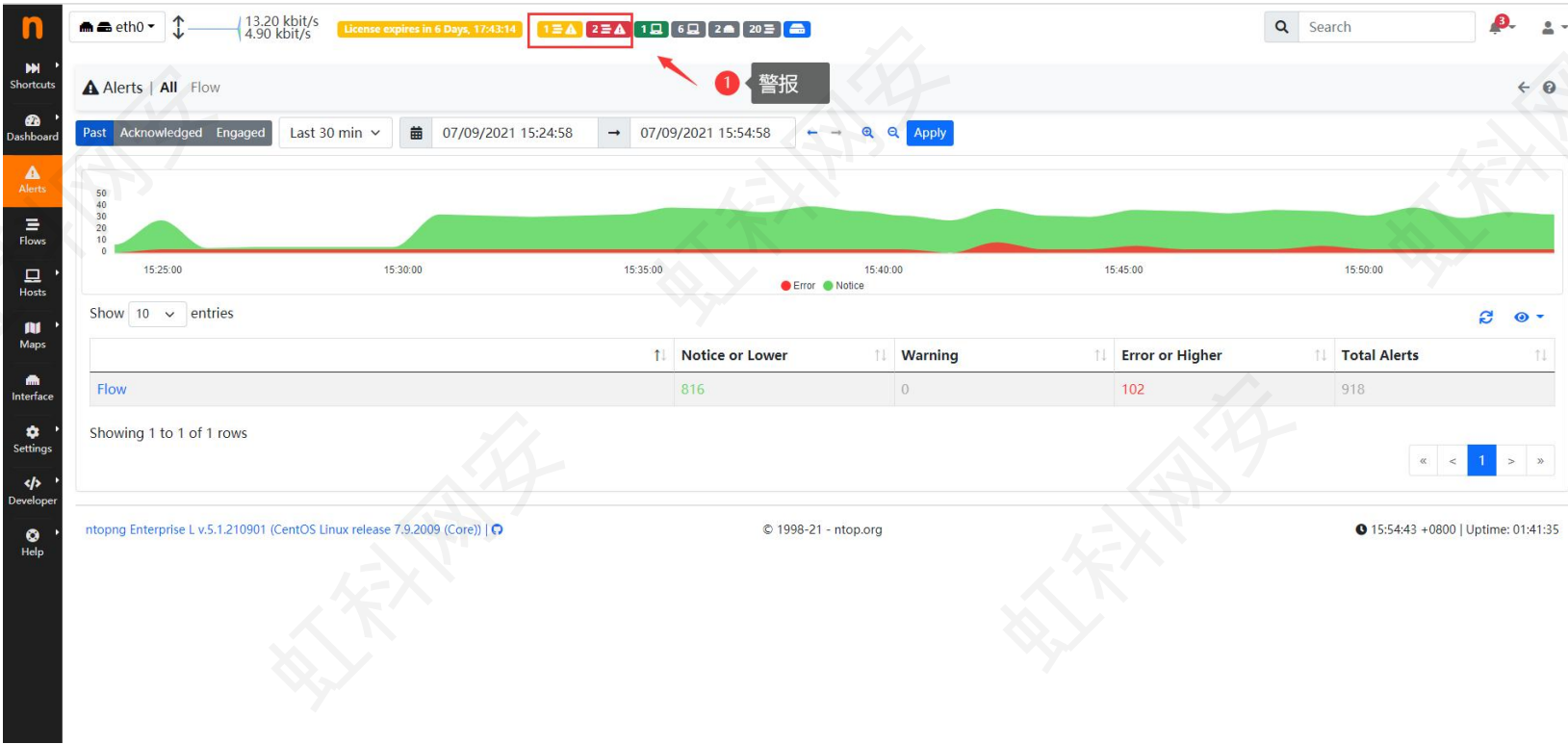
Name	Category	Description	Values	Action
Countries Contacts Alert	🛡️	Trigger an alert when the number of different countries contacted exceeds the threshold	> 100 Contacts (Minute)	🛑 ✎
Dangerous Host	🛡️	Trigger an alert when an host crosses the configured score threshold for more than 5 consecutive minutes	> 1000 Score (Minute)	🛑 ✎
DNS Server Contacts Alert	🛡️	Trigger an alert when the number of different DNS servers contacted exceeds the threshold	> 5 Contacts (Minute)	🛑 ✎
DNS Traffic Alert	🛡️	Trigger an alert when layer 2 Bytes delta (sent + received) for DNS traffic exceeds the threshold	> (1 MB)	🛑 ✎
Alert	🛡️	Trigger an alert when the number of contacted Domain Names is greater then a certain threshold	> 250 Contacts (Minute)	🛑 ✎
	🛡️	Trigger an alert when the new client/server Flows/sec exceeds the threshold	> 256 Flows/sec (Minute)	🛑 ✎
	🛡️	Detects anomalies in active flows number		🛑 ✎
	🛡️	Trigger an alert when the number of different NTP servers contacted exceeds the threshold	> 5 Contacts (Minute)	🛑 ✎
	🛡️	Trigger an alert when the Layer 2 bytes delta (sent + received) for NTP traffic exceeds the threshold	> (1 MB)	🛑 ✎
	🛡️	Trigger an alert when the Layer 2 bytes delta (sent + received) for P2P traffic exceeds the threshold		🛑 ✎

[返回主页](#)

ntopng 应用示例

● 警报查询: Alert

ntopng提供了常见流量异常警告功能，通过左侧菜单选择Alert查看当前和历史所有警告信息。并可根据时间范围，警报类型和危险等级等进行高级的过滤。



The screenshot shows the ntopng Alerts page. At the top, there's a navigation bar with 'Alerts | All | Flow' and a search bar. Below that, there are filters for 'Past', 'Acknowledged', 'Engaged', and 'Last 30 min'. A date range is set to '07/09/2021 15:24:58' to '07/09/2021 15:54:58'. A chart shows the number of alerts over time, with a red line for 'Error' and a green area for 'Notice'. Below the chart is a table with columns for 'Notice or Lower', 'Warning', 'Error or Higher', and 'Total Alerts'. The table shows 816 Notice or Lower alerts, 0 Warning alerts, 102 Error or Higher alerts, and a total of 918 alerts. The footer shows 'ntopng Enterprise L v.5.1.210901 (CentOS Linux release 7.9.2009 (Core)) | © 1998-21 - ntop.org' and '15:54:43 +0800 | Uptime: 01:41:35'.

	Notice or Lower	Warning	Error or Higher	Total Alerts
Flow	816	0	102	918

[\[返回主页\]](#)

ntopng 应用示例

● 警报查询: Alert

通过左侧菜单选择Alert查看当前和历史所有警告信息。并可根据时间范围，警报类型和危险等级等进行高级的过滤。

The screenshot shows the ntopng Alerts page. It includes a sidebar with navigation options like Alerts, Flows, Hosts, Maps, Interface, Settings, Developer, and Help. The main area features a 'Filters' section with a date range selector (07/09/2021 15:28:05 to 07/09/2021 15:58:05) and a 'Filters' button. Below this is a line graph showing alert levels over time, with a legend for 'Error' (red) and 'Notice' (green). To the right of the graph are two summary boxes: 'Top Hosts' and 'Top Alerts'. The 'Top Alerts' box lists: HTTP Numeric IP Host (86.8%), Suspicious DGA Domain (10.4%), and Unidirectional UDP Traff... (1.2%). Below the graph is a table of alert entries. The table has columns for Date/Time, Score, Application, Alert, Flow, and Actions. The first row shows an alert at 15:28:24 with a score of 100, Application UDP:DNS, and Alert Suspicious DGA Domain. The Actions column for each row contains icons for settings, search, refresh, and delete. Annotations with red arrows and numbers 1-5 point to various UI elements: 1 points to the legend, 2 points to the graph area, 3 points to the 'Add Filter' button, 4 points to the 'View Details' icon, and 5 points to the 'Alert Settings' icon.

Date/Time	Score	Application	Alert	Flow	Actions
15:28:24	100	UDP:DNS	Suspicious DGA Domain	izwz9bhxg6t9vtmz3oggz3z:51487	[Settings] [Search] [Refresh] [Delete]
15:28:24	100	UDP:DNS	Suspicious DGA Domain	izwz9bhxg6t9vtmz3oggz3z:34891	[Settings] [Search] [Refresh] [Delete]
15:28:24	110	TCP:TLS	Suspicious DGA Domain	izwz9bhxg6t9vtmz3oggz3z:34348	[Settings] [Search] [Refresh] [Delete]
15:28:25	10	TCP:HTTP.ntop	HTTP Numeric IP Host	220.33.209.222.broad.cd...:41347	[Settings] [Search] [Refresh] [Delete]
15:29:22	110	TCP:TLS	Suspicious DGA Domain	izwz9bhxg6t9vtmz3oggz3z:34390	[Settings] [Search] [Refresh] [Delete]
15:29:22	100	UDP:DNS	Suspicious DGA Domain	izwz9bhxg6t9vtmz3oggz3z:39321	[Settings] [Search] [Refresh] [Delete]
15:29:22	100	UDP:DNS	Suspicious DGA Domain	izwz9bhxg6t9vtmz3oggz3z:49091	[Settings] [Search] [Refresh] [Delete]
15:29:25	10	TCP:HTTP.ntop	HTTP Numeric IP Host	220.33.209.222.broad.cd...:43782	[Settings] [Search] [Refresh] [Delete]

[\[返回主页\]](#)

ntopng 应用示例

历史流回溯分析

[\[返回主页\]](#)

ntopng 应用示例

● 历史数据存储设置：Setting->Preferences->Data Retention

设置数据存储时间将决定历史图表的回溯时长以及Flow数据的流存时长。




[\[返回主页\]](#)

ntopng 应用示例

● 时间序列设置：Setting->Preferences->Timeserise

时间序列下拉选项中有许多可选项，选择那些模块需要添加时间序列，例如为本地主机添加时间序列设置，这意味着我们可以为每个本地主机单独创建历史图表，只有设置了时间序列，才能生成历史流量时序图。



Local Hosts Timeseries

Host Timeseries Off Light Full
Enable full host timeseries creation (full), limit it to bytes and score (light), or turn it off.

One-Way Traffic Timeseries
Toggle the creation of timeseries for one-way traffic. One-way traffic is often generated by remote hosts performing probing, so it is advisable to keep this disabled.

Layer-7 Applications None Per Application Per Category Both
Toggle the creation of Layer-7 application timeseries. Creating a timeseries per application requires more disk space and extra I/O and, in general, it is not needed.

Devices Timeseries

Traffic
Toggle the creation of bytes and packets timeseries.

Probes Timeseries

Probes
Toggle the creation of timeseries for system probes such as the Active Monitoring and the Redis monitor.

Other Timeseries

Flow Probes
Toggle the creation of bytes timeseries for each port of the remote device as received through ZMQ

[\[返回主页\]](#)

ntopng 应用示例

● 历史浏览器: Historical Explorer

历史浏览器允许提取特定时间段的历史流信息，可以添加多种过滤器根据IP应用程序筛选感兴趣的流量，根据设置最大可存储一年或以上历史数据。

The screenshot shows the ntopng Historical Explorer interface. At the top, there is a search bar and a time range selector. The time range is set to 'Last 30 min' and '07/09/2021 09:46:27' to '07/09/2021 10:16:27'. A search button is labeled '搜索' (Search). A filter icon is labeled '添加过滤器' (Add Filter). The main table displays network flow data with columns for Client IP, Client Port, Server Port, Protocol, Application, Score, Pkts, Bytes, Thpt, Begin, End, Client ASN, and Server ASN. The table contains 10 rows of data, all showing HTTP traffic from 222.209.33.220 to various ports on izwz9bhxg6t9... servers. A download button is labeled '下载' (Download). At the bottom, there are buttons for 'Get permanent link' and 'Download Records'.

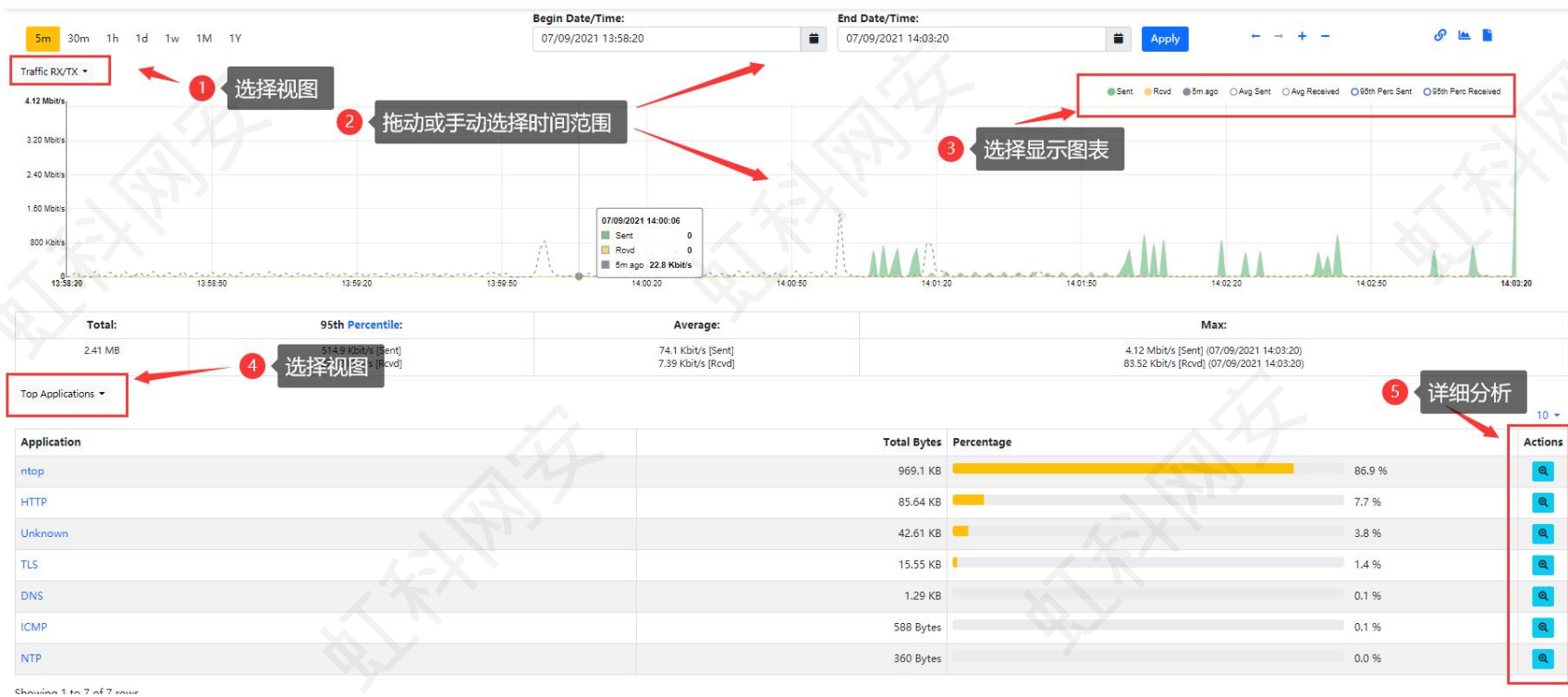
Client IP	Client Port	Srv Port	Protocol	Application	Score	Pkts	Bytes	Thpt	Begin	End	Client ASN	Srv ASN
222.209.33.220	42949	3000	TCP	HTTP	20	1,318 Pkts	1.28 MB	3.58 Mbit/s	09/07/21 09:48:28	09/07/21 09:48:30	4134 (Chinanet)	No ASN
222.209.33.220	42758	3000	TCP	HTTP	20	1,234 Pkts	1.2 MB	2.53 Mbit/s	09/07/21 09:48:28	09/07/21 09:48:31	4134 (Chinanet)	No ASN
222.209.33.220	41860	3000	TCP	HTTP	20	159 Pkts	161.25 KB	1.32 Mbit/s	09/07/21 09:48:28	09/07/21 09:48:28	4134 (Chinanet)	No ASN
222.209.33.220	43844	3000	TCP	HTTP	20	142 Pkts	138.88 KB	1.14 Mbit/s	09/07/21 09:48:55	09/07/21 09:48:55	4134 (Chinanet)	No ASN
222.209.33.220	43594	3000	TCP	HTTP.ntop	10	87 Pkts	83.79 KB	686.45 kbit/s	09/07/21 09:57:01	09/07/21 09:57:01	4134 (Chinanet)	No ASN
222.209.33.220	43272	3000	TCP	HTTP	20	94 Pkts	83.35 KB	682.79 kbit/s	09/07/21 09:48:29	09/07/21 09:48:29	4134 (Chinanet)	No ASN
222.209.33.220	44743	3000	TCP	HTTP	20	87 Pkts	79.41 KB	650.5 kbit/s	09/07/21 09:48:31	09/07/21 09:48:31	4134 (Chinanet)	No ASN
222.209.33.220	41413	3000	TCP	HTTP.ntop	10	65 Pkts	60.58 KB	496.25 kbit/s	09/07/21 09:53:29	09/07/21 09:53:29	4134 (Chinanet)	No ASN
222.209.33.220	42123	3000	TCP	HTTP	20	66 Pkts	59.81 KB	489.99 kbit/s	09/07/21 09:48:28	09/07/21 09:48:28	4134 (Chinanet)	No ASN
222.209.33.220	44292	3000	TCP	HTTP.ntop	10	121 Pkts	109.79 KB	449.68 kbit/s	09/07/21 10:01:38	09/07/21 10:01:39	4134 (Chinanet)	No ASN

[\[返回主页\]](#)

ntopng 应用示例

● 接口历史流量回溯分析: Interface-


接口历史流分析界面，该提供详细的历史流量统计信息。用户可以自由选择需要的分析时间段，基于协议，主机对流量进行过滤分析历史流数据。

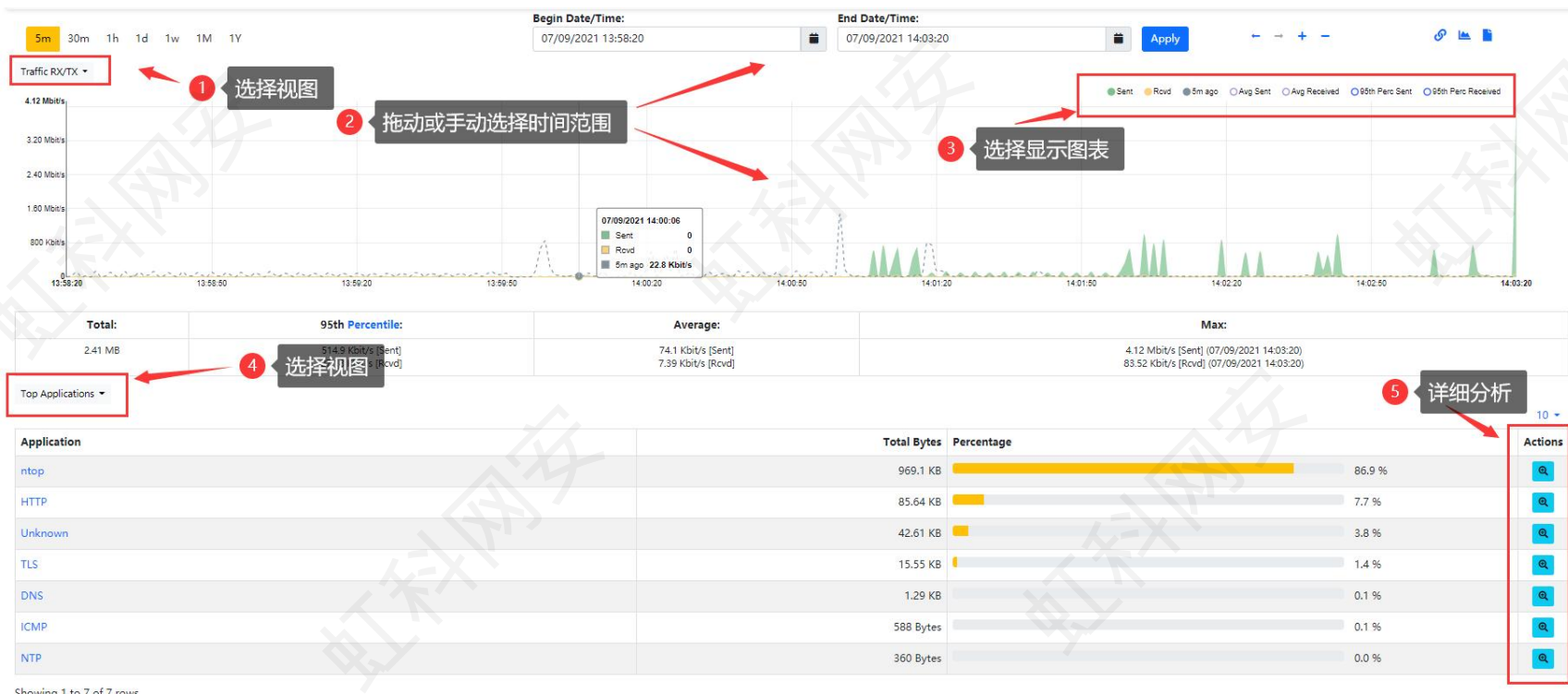


[\[返回主页\]](#)

ntopng 应用示例

● 主机历史流量回溯分析：主机详细->

在主机详细页面也提供了历史流量分析功能，选择  进行主机级别的历史流量分析，界面与接口历史流量图表基本相同，不同的是这是针对特定IP的历史流量分析，



[\[返回主页\]](#)

ntopng 应用示例

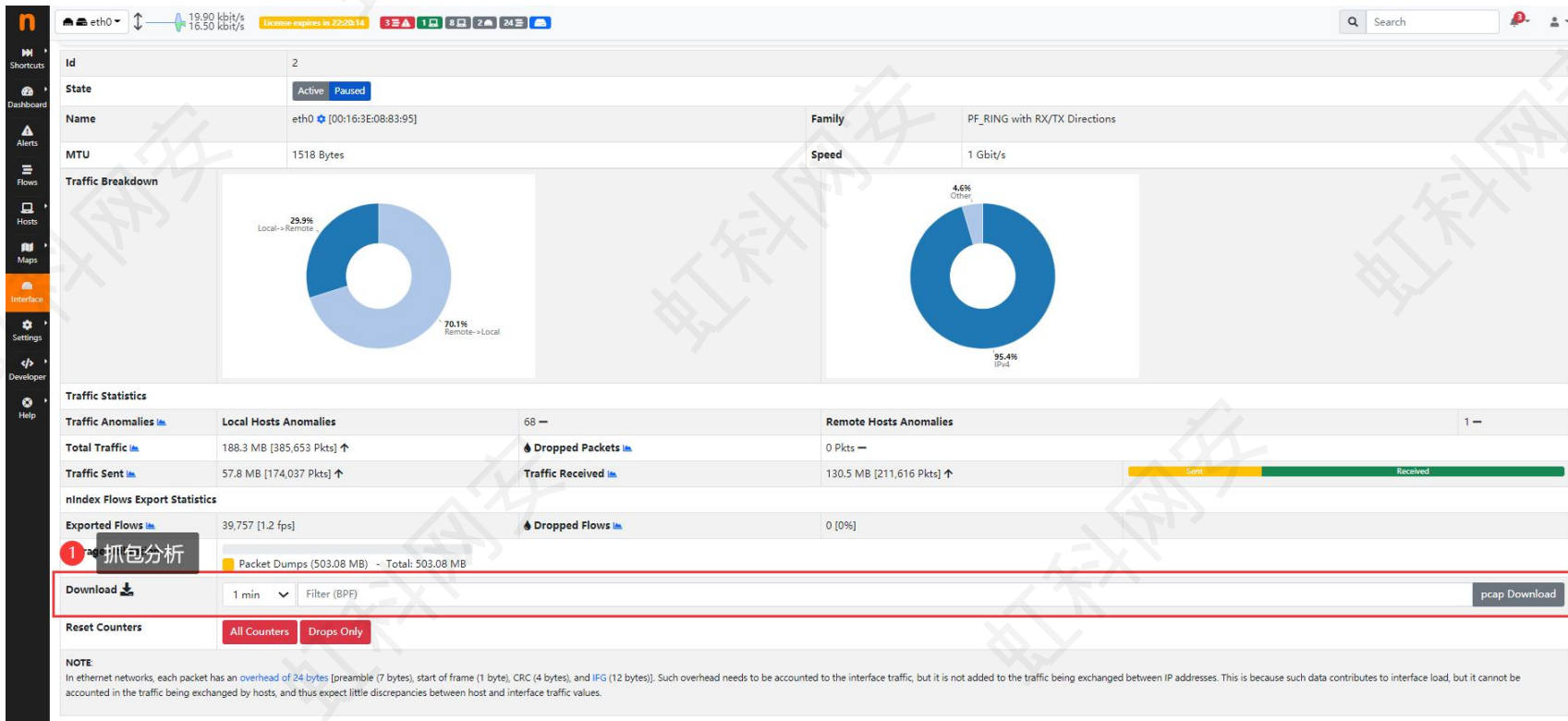
实时抓包分析

[\[返回主页\]](#)

ntopng 应用示例

● 接口抓包分析：Interface->Home

在接口详细Home页面底部提供实时抓包分析功能，可以设置BFP过滤器抓取感兴趣的流量。



抓包分析

Download 1 min Filter (BPF) pcap Download

Reset Counters All Counters Drops Only

NOTE
In ethernet networks, each packet has an overhead of 24 bytes [preamble (7 bytes), start of frame (1 byte), CRC (4 bytes), and IPG (12 bytes)]. Such overhead needs to be accounted to the interface traffic, but it is not added to the traffic being exchanged between IP addresses. This is because such data contributes to interface load, but it cannot be accounted in the traffic being exchanged by hosts, and thus expect little discrepancies between host and interface traffic values.

[\[返回主页\]](#)

ntopng 应用示例

● 主机抓包分分析：主机详情>Home

在主机详情Home页面底部也提供实时抓包分析功能，不同的是这里只抓取该主机IP的流量。

The screenshot shows the ntopng interface for a host. The main content area displays various statistics and monitoring tools. At the bottom left of this area, a button labeled '抓包分析' (Packet Capture Analysis) is highlighted with a red box and a red circle containing the number 1. Below this button is a 'Download' section with a 'JSON' link and a 'pcap Download' button. The interface also shows a search bar at the top right and a sidebar on the left with navigation options like 'Hosts', 'Maps', and 'Interface'.

[\[返回主页\]](#)

ntopng 应用示例

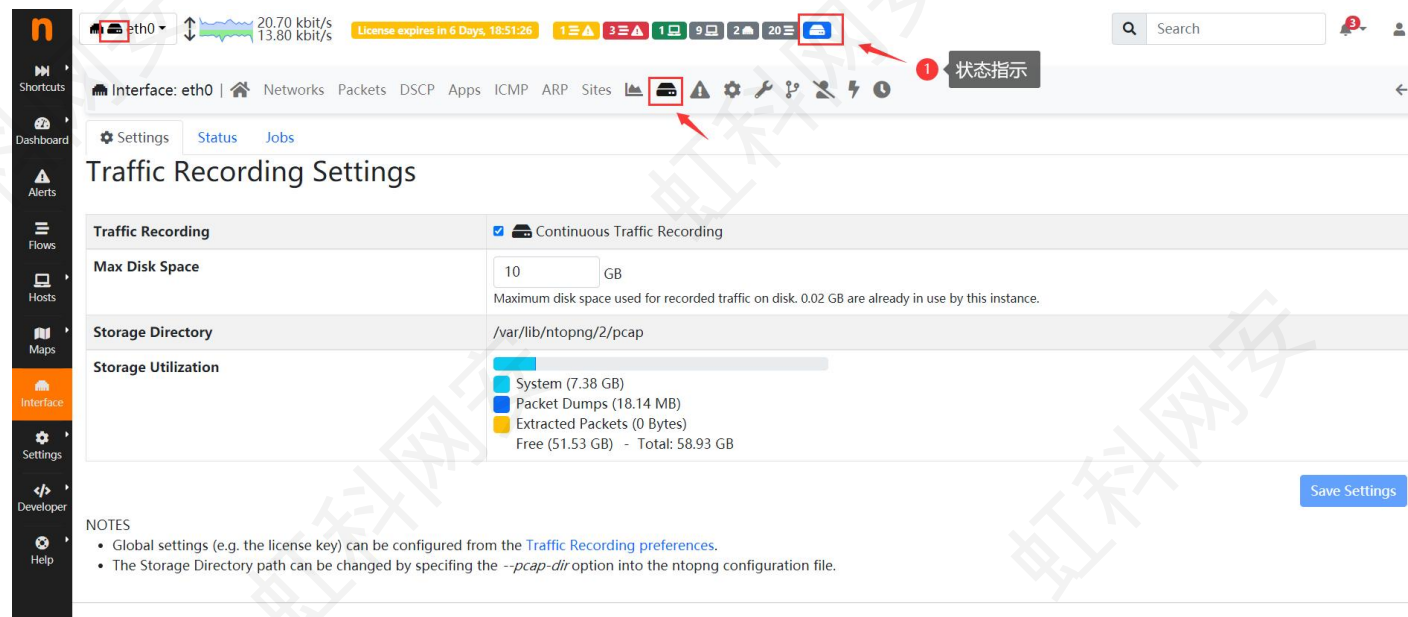
全流量回溯分析

[\[返回主页\]](#)

ntopng 应用示例

● 连续流量记录: Interface->

当你拥有 *n2disk* 许可证时，可以启动连续流量记录功能这样将存储所有接口流量，设置最大流量记录空间，当流量超出设置空间时，最开始的流量将被删除。点击保存设置开始记录，设置成功顶部状态指示为蓝色，否则为红色。同时接口处也将增加连续流量记录的图标。



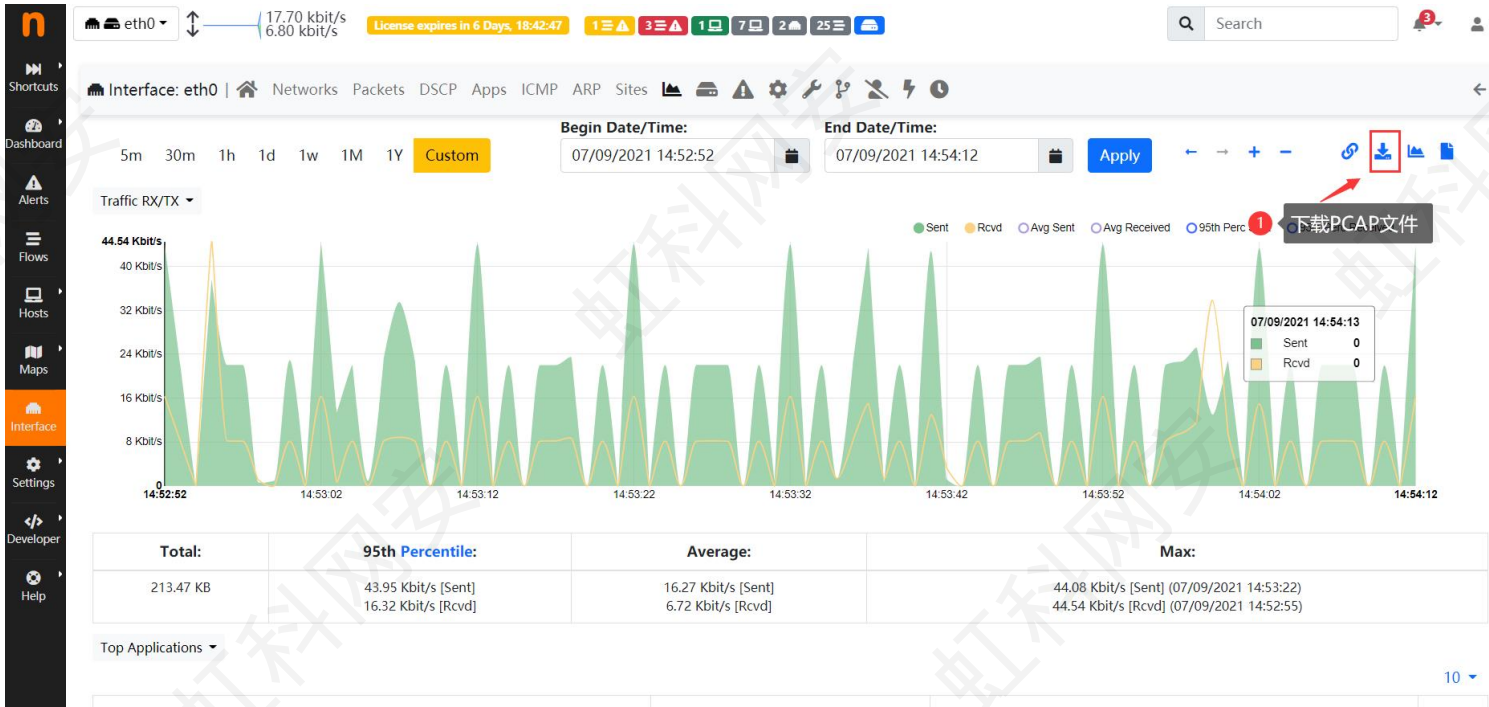
The screenshot shows the ntopng web interface. At the top, the interface for interface `eth0` is visible, showing traffic statistics (20.70 kbit/s up, 13.80 kbit/s down) and a license expiration notice. A red box highlights the traffic recording icon in the top navigation bar, with a red arrow pointing to a tooltip labeled "状态指示" (Status Indicator). Below this, the "Traffic Recording Settings" page is displayed. The "Traffic Recording" checkbox is checked, and "Continuous Traffic Recording" is selected. The "Max Disk Space" is set to 10 GB, with a note that 0.02 GB is already in use. The "Storage Directory" is `/var/lib/ntopng/2/pcap`. The "Storage Utilization" section shows a bar chart with the following breakdown: System (7.38 GB), Packet Dumps (18.14 MB), and Extracted Packets (0 Bytes). The total free space is 51.53 GB, and the total used space is 58.93 GB. A "Save Settings" button is located at the bottom right of the settings form. Below the settings, there are "NOTES" regarding global settings and the `--pcap-dir` option.

[\[返回主页\]](#)

ntopng 应用示例

● 全流量回溯分析: Interface

配置成功后可以在接口历史图表，或者主机历史图表选择时间段，下载原始流量PCAP文件。



[\[返回主页\]](#)

ntopng 应用示例

自定义应用

[\[返回主页\]](#)

ntopng 应用示例

● 自定义应用程序：Setting->Applications and Categories

要启用启用此功能，ntopng 配置文件应该添加 `-ndpi-protocols=/var/lib/ntopng/protos.txt`选项启动。如果您已经有 protos 文件，请将其移动到/var/lib/ntopng/protos.txt并运行，然后在Setting->Applications and Categories点击添加。

Application	Category	Custom Rules	Actions
Zoom	Video		Edit Rules
ZeroMQ	RPC		Edit Rules
Zattoo	Video		Edit Rules
	Network		Edit Rules
	Network		Edit Rules
	Media		Edit Rules
	Media		Edit Rules

[\[返回主页\]](#)

ntopng 应用示例

● 自定义应用程序：Setting->Applications and Categories

通过单击 **+** 或者 **Edit Rules** 按钮，可以直接从 GUI 编辑应用程序规则并添加新协议。需要注意的是，规则和新协议只会在 ntopng 重新启动后创建和应用。目前支持根据 IP，网段，端口和字符串匹配规则。

Add Custom Application ×

Application Name

Google

Custom Rules

```
220.221.12.235
tcp:2355
google.com
```

NOTES

- Each rule must be put on a separate line
- Rules can be either domain names, IPv4 addresses or TCP/UDP port ranges
- Port range examples: "udp:443", "tcp:1230-1235"
- Domain names are interpreted as substring to be matched.
E.g. "ntop.org" will match "mail.ntop.org" and "ntop.org.example.com"

[\[返回主页\]](#)

ntopng 应用示例

SNMP监控

[\[返回主页\]](#)

ntopng 应用示例

● 启动SNMP时间序列: Setting->Preferences->SNMP

在首选项->SNMP中可以设置启用SNMP时间序列，这将为每个SNMP接口创建时序表。

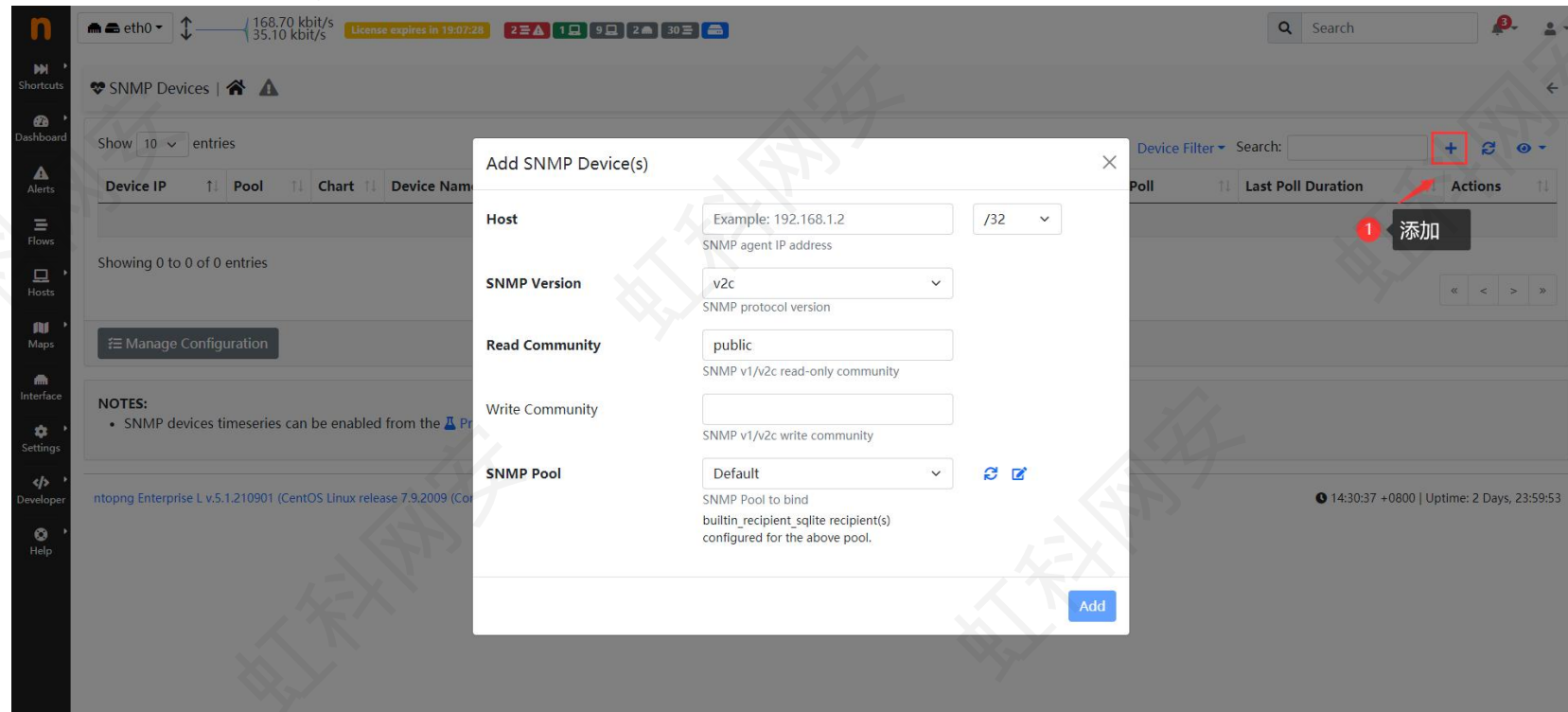
The screenshot shows the ntopng web interface. The top navigation bar includes a search box, a notification bell with 3 alerts, and a user profile icon. The main content area is titled 'Runtime Preferences' and features a search bar for preferences. A left sidebar lists various settings categories, with 'Settings' highlighted in orange. The 'SNMP' category is selected, displaying several configuration options: 'SNMP Devices Timeseries' (a toggle switch that is turned on, highlighted with a red box and a callout bubble labeled '1 启用时间序列'), 'Default SNMP Version' (set to v2c), 'Default SNMP Community' (set to public), 'SNMP Agent Response Timeout' (set to 3 seconds), and 'SNMP Debug' (a toggle switch that is turned off). A 'Save' button is located at the bottom right of the settings panel.

[\[返回主页\]](#)

ntopng 应用示例

● 添加SNMP设备: Shortcuts->SNMP

在SNMP监控界面点击添加即可添加SNMP设备。

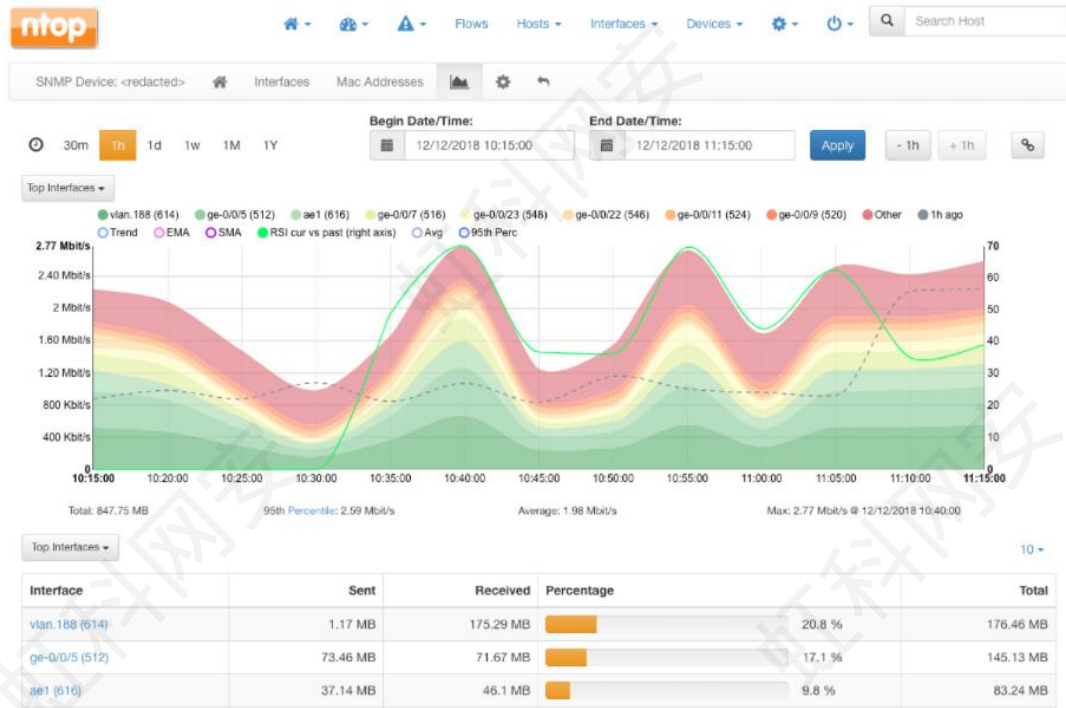


[\[返回主页\]](#)

ntopng 应用示例

● SNMP历史图表: 

最有用的历史图表将显示特定时间范围内最高接口流量速度的堆叠图表。在图表正下方，还显示了同一时间范围内的接口总数。



[\[返回主页\]](#)

ntopng 应用示例

- SNMP接口列表:

设备接口状态现在显示在动态加载的分页表中。

	Index	Interface Name	VLAN	Speed	Status	MACs	In Bytes	Out Bytes	In Discards	Throughput	Last Change
Info	535	ge-0/0/19	188	1.0 Gbit	Up		2.74 GB	2.43 GB		69.85 Mbit/s	01:27:13
Info	600	ge-0/0/1		1.0 Gbit	Up		1.96 GB	885.97 MB		47.83 Mbit/s	16:56:34
Info	595	vlan.2		1.0 Gbit	Up		1.52 GB	596.43 MB		17.15 Mbit/s	16 days, 13:27:05
Info	604	ge-0/1/0		1.0 Gbit	Up		1.51 GB	381.28 MB		17.13 Mbit/s	16 days, 13:27:01
Info	511	ge-0/0/7		1.0 Gbit	Up		1.08 GB	2.93 GB		6.0 Mbit/s	27:36
Info	551	ge-0/0/33	188	1.0 Gbit	Up		3.91 GB	1.37 GB		5.24 Mbit/s	16 days, 13:27:00
Info	531	ge-0/0/17	188	1.0 Gbit	Up		702.49 MB	3.26 GB		3.05 Mbit/s	16 days, 13:27:05
Info	519	ge-0/0/11	188	1.0 Gbit	Up		790.15 MB	1.7 GB		856.66 kbit/s	1 day, 02:14:56
Info	6	lo0			Up		1.16 GB	1.16 GB		537.06 kbit/s	16 days, 13:27:18
Info	592	ge-0/0/22		1.0 Gbit	Up		1.29 GB	3.69 GB		256.69 kbit/s	01:29:01

[\[返回主页\]](#)

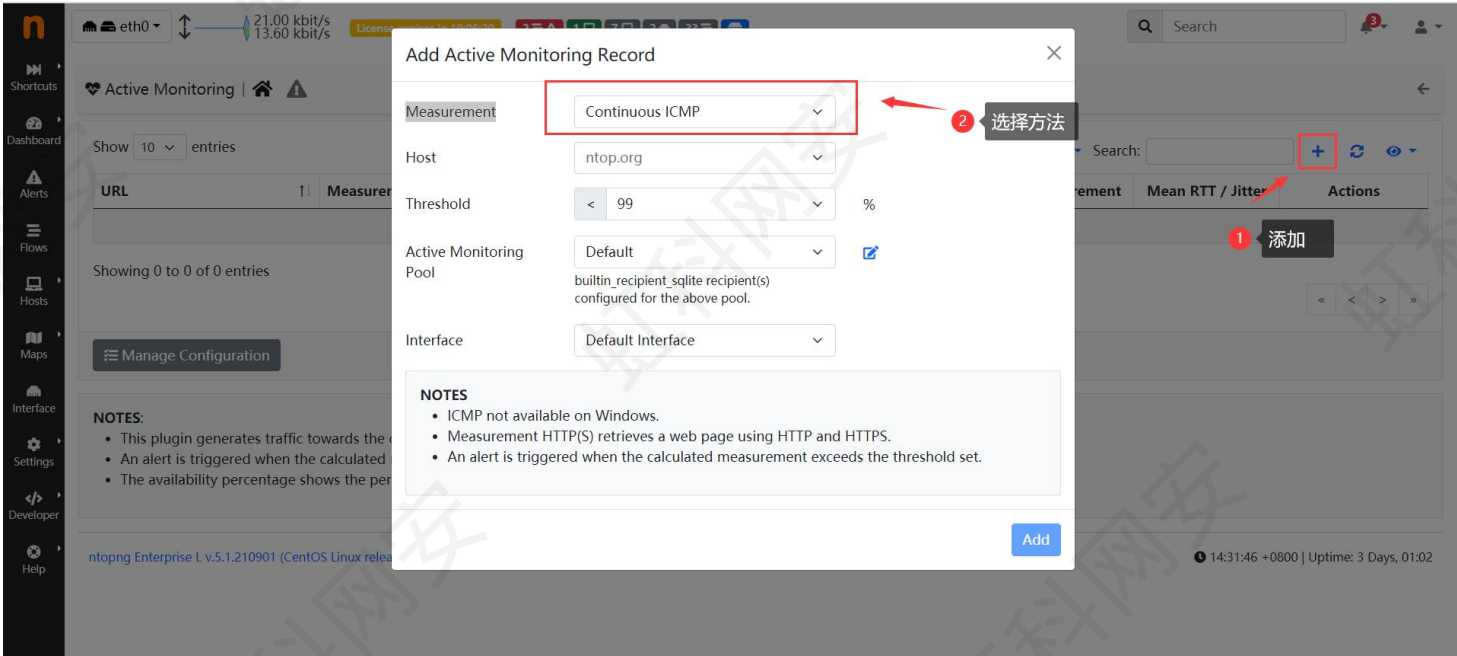
ntopng 应用示例

活动监控

[\[返回主页\]](#)

ntopng 应用示例

● 添加活动监控: Shortcuts->SNMP

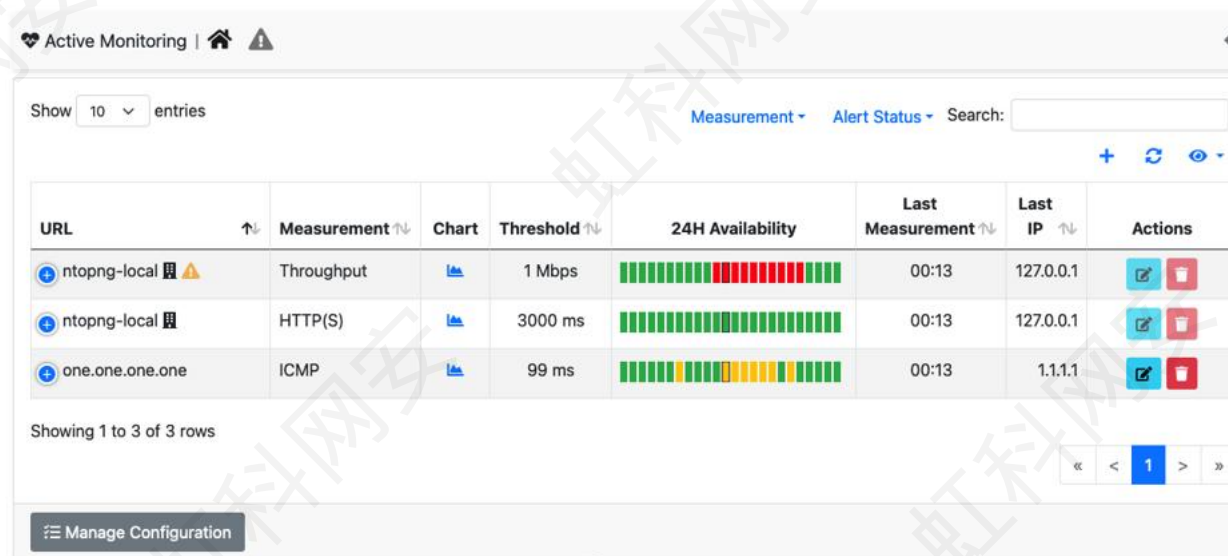


ntopng 应用示例

● 活动监控: Shortcuts-> Active Monitoring

活动监视器每分钟探测配置主机以检查:

- ICMP: 检查主机 IP 可达性
- HTTP 和 HTTPS: 检查主机 Web 服务器的功能
- Speedtest: 检查互联网带宽



The screenshot shows the ntopng Active Monitoring interface. At the top, it says "Active Monitoring" with a home icon and a warning icon. Below that, there are controls for "Show 10 entries", "Measurement", "Alert Status", and a search box. The main part of the interface is a table with the following columns: URL, Measurement, Chart, Threshold, 24H Availability, Last Measurement, Last IP, and Actions. There are three rows of data:

URL	Measurement	Chart	Threshold	24H Availability	Last Measurement	Last IP	Actions
ntopng-local	Throughput	[Chart Icon]	1 Mbps	[Availability Bar]	00:13	127.0.0.1	[Action Icons]
ntopng-local	HTTP(S)	[Chart Icon]	3000 ms	[Availability Bar]	00:13	127.0.0.1	[Action Icons]
one.one.one.one	ICMP	[Chart Icon]	99 ms	[Availability Bar]	00:13	1.1.1.1	[Action Icons]

Below the table, it says "Showing 1 to 3 of 3 rows" and there are navigation buttons. At the bottom left, there is a "Manage Configuration" button.

[\[返回主页\]](#)

ntopng 应用示例

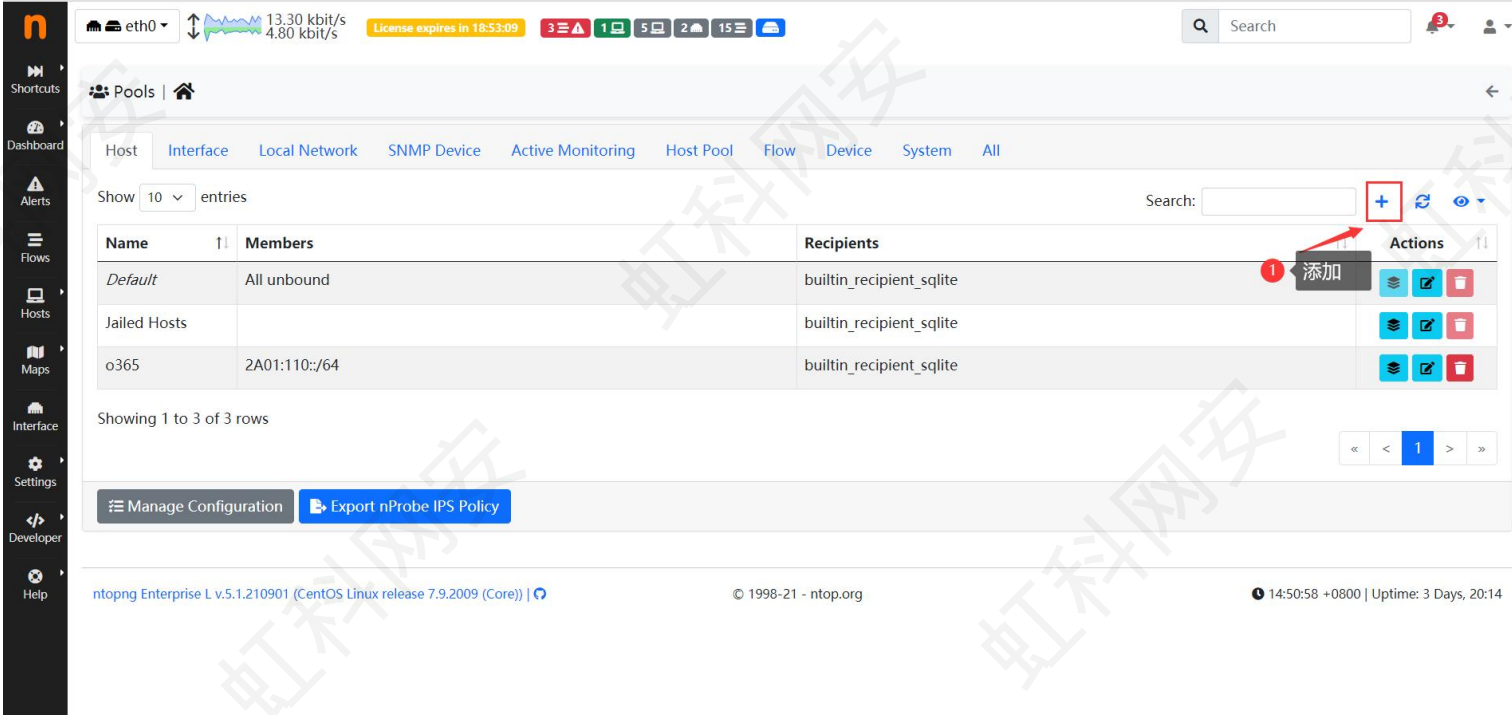
主机池划分

[\[返回主页\]](#)

ntopng 应用示例

- 主机池划分: Shortcuts-> Pools


主机池是主机的逻辑组，可以根据IPv4/IPv6网段，MAC地址等划分自定义主机池，对每个主机池生成单独的流量统计信息，可以在，Shortcuts-> Pools 点击 **+** 添加主机池。




[\[返回主页\]](#)

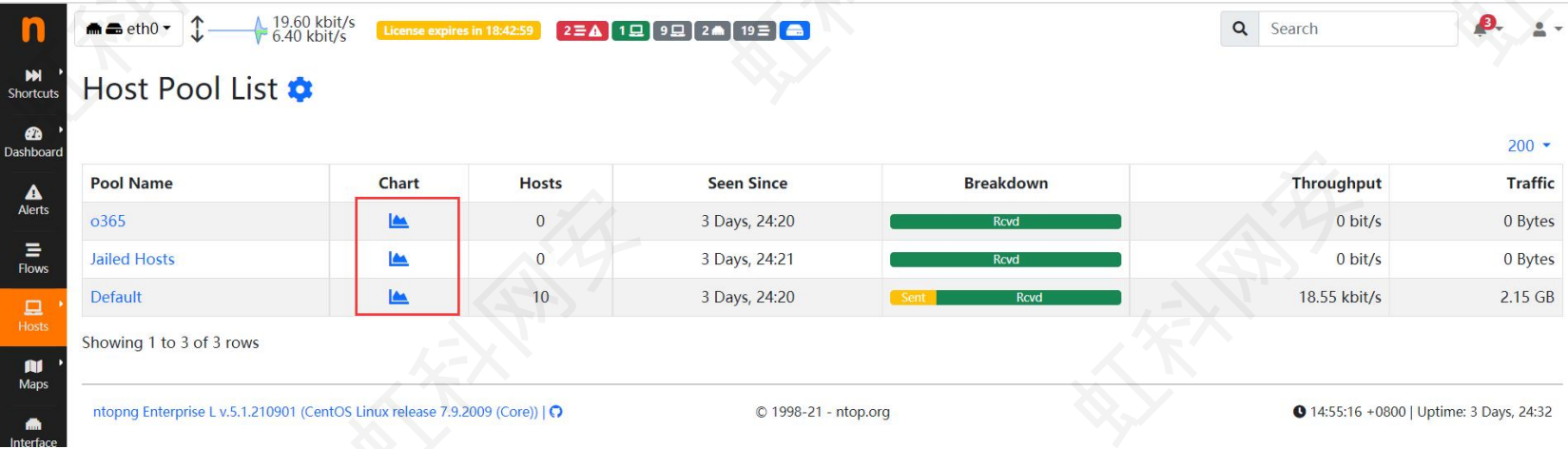
ntopng 应用示例

- 主机池添加时间序列: Settings-> Preferences->Timeserise




为主机池添加时间序列可以为每个主机池创建历史流量时序视图，可在Hosts->Host Pool查看主机池流量使用详细，点击主机名或者历史图表  查看更多详细统计信息。

Host Pools 

Toggle the creation of bytes and applications timeseries for defined host pools.



The screenshot shows the ntopng Host Pool List interface. At the top, there is a status bar with network statistics (eth0, 19.60 kbit/s sent, 6.40 kbit/s received), a license expiration warning (License expires in 18:42:59), and several alert icons. Below the status bar is a search bar and a user profile icon. The main content area is titled "Host Pool List" and contains a table with the following data:

Pool Name	Chart	Hosts	Seen Since	Breakdown	Throughput	Traffic
o365		0	3 Days, 24:20	Rcvd	0 bit/s	0 Bytes
Jailed Hosts		0	3 Days, 24:21	Rcvd	0 bit/s	0 Bytes
Default		10	3 Days, 24:20	Sent Rcvd	18.55 kbit/s	2.15 GB

Showing 1 to 3 of 3 rows

Footer: ntopng Enterprise L v.5.1.210901 (CentOS Linux release 7.9.2009 (Core)) | © 1998-21 - ntop.org | 14:55:16 +0800 | Uptime: 3 Days, 24:32

[\[返回主页\]](#)